RIESGOS, AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS DE INFORMACIÓN GEOGRÁFICA

DUVAN ERNESTO CASTRO BOLAÑOS
ÁNGELA DAYANA ROJAS MORA

UNIVERSIDAD CATÓLICA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
MODALIDAD TRABAJO DE INVESTIGACION
BOGOTÁ
2013

RIESGOS, AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS DE INFORMACIÓN GEOGRÁFICA

DUVAN ERNESTO CASTRO BOLAÑOS
ÁNGELA DAYANA ROJAS MORA

Trabajo de grado para optar al título de
Ingeniero de Sistemas

Director
Jorge Enrique Carrillo Contreras
Ingeniero de Sistemas Especialista en Diseño y Soluciones Telemáticas

UNIVERSIDAD CATÓLICA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
MODALIDAD TRABAJO DE INVESTIGACION
BOGOTÁ
2013

Nota de Aceptación:

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C., Noviembre 2013

AGRADECIMIENTOS

En primer lugar agradecemos a Dios por todas las bendiciones que nos otorgó a lo largo del transcurso del proyecto y de la carrera.

A nuestras familias, por brindarnos su incondicional apoyo, por habernos formado con valores, y por las tantas pruebas de amor sin las cuales no hubiera sido posible afrontar este gran reto.

De manera especial a las orientaciones del Ingeniero Jorge E. Carrillo, quien estuvo con nosotros de principio a fin en el desarrollo del proyecto, compartiéndonos sus conocimientos en el tema.

CONTENIDO

pág.

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

pág.

pág.

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO: es todo elemento o material digital, físico o humano que puede ser afectado y que requiere protección
AMENAZA: es el evento que puede afectar los activos de la organización.
ESTIMACIÓN DEL RIESGO: es el proceso que permite asignar valores para determinar la probabilidad y las consecuencias de un riesgo sobre un activo.
IDENTIFICACIÓN DEL RIESGO: es el proceso que permite encontrar, enumerar y caracterizar los activos de riesgo.
IMPACTO: es el efecto que puede generar la materialización de una amenaza sobre un activo.
ISO/IEC 27001: es la norma internacional auditable que da los parámetros para definir los requisitos para gestionar la seguridad de la información (SGSI).
ISO/IEC 27005: es la norma que proporciona las directrices para la gestión de riesgos en la seguridad de la información
MATRIZ: es la unificación de elementos en forma rectangular, que permite realizar algunas operaciones matemáticas para hacer análisis y estudios de los resultados brindados.
RIESGO: es el impacto que se puede producir sobre un activo.
SISTEMA DE INFORMACIÓN GEOGRÁFICA: es la unificación de software hardware y datos geográficos.
SISTEMA DE POSICIONAMIENTO GLOBAL: es el sistema de posicionamiento por medio de satélites que se encarga de recoger y brindar información para los Sistemas de Información Geográfica.
VULNERABILIDAD: es la debilidad que puede presentar un activo sobre una amenaza.

RESUMEN

En la actualidad los sistemas de información geográfica han tomado valor en las diferentes organizaciones que manejan recursos de posición y ubicación geográficos. La gestión de estos sistemas requiere como todo sistema de información una definición de normas de uso y administración adecuadas.

El presente trabajo se orienta a realizar un análisis de riesgos de un sistema de información geográfica, en el que se tratan las técnicas de seguridad de la norma ISO/IEC 27001:2005, y la gestión de riesgos de la seguridad de la norma ISO 27005.

Se pretende identificar los riesgos con mayor probabilidad de suceso ante un análisis de impacto/probabilidad, y así mismo establecer los controles o medidas de protección correspondientes al riesgo para proteger los activos de la organización.

ABSTRACT

At present, geographic information systems have taken different value in organizations that handle position resources and geographical location. The management of these systems requires, as any information system, a definition of terms of use and appropriate management.

The present study aims to conduct a risk analysis of a geographic information system, which are discussed security techniques of ISO / IEC 27001:2005 standard, risk management and security of ISO 27005 standard.

The aim is to identify the risks most likely event to an impact analysis / probability, and likewise set the controls or protective measures to protect risk assets of the organization.

INTRODUCCIÓN

La investigación que se va a realizar tiene como fin dar a conocer las debilidades que presentan los sistemas de información geográfica (SIG), las amenazas a las que está expuesto y los impactos relativos del riesgo.

Los sistemas de información geográfica son muy populares en la actualidad y a su vez de gran importancia en la sociedad, especialmente en los ámbitos donde se requiere el manejo de datos geográficos. Un SIG es definido como un conjunto de hardware, software, datos, recursos humanos y metodologías para el almacenamiento, análisis, transformación y presentación de toda la información geográfica y sus atributos.

La implementación de un SIG debe abarcar las medidas de seguridad que protejan los datos contra cualquier situación de riesgo, esto serán las buenas prácticas de seguridad que utilicen las organizaciones.

Este proyecto pretende analizar cómo es asegurada la información de un SIG hoy en día y que tipos de vulnerabilidades existen frente a este sistema

1. GENERALIDADES

1.1 ANTECEDENTES

Se ha realizado varios estudios sobre las vulnerabilidades de los sistemas de información, estos estudios han sido plasmados en documentos por diferentes universidades en diferentes partes de mundo, los estudios más relevantes para esta investigación son: Documento científico de Carnegie Mellon University y la compañía Coherent Navigation sobre GPS Software Attacks; el articulo GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques realizado por Position Location and Navigation (PLAN) Group, Schulich School of Engineering, University of Calgary, 2500 University Drive,NW, Calgary, AB, Canada T2N 1N4; el documento A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing realizado por el laboratorio Los Alamos National Laboratory; el documento Secure Tracking for Critical Applications: Communications, GPS and Future Galileo Services realizado University of Queensland, Australia y la compañía Qascom S.r.l., Italy; la tesis Security mechanisms for positioning systems - enhancing the security of eLoran elaborada en la universidad Ruhr-Universit¨at Bochum de Alemania; la tesis Detection of spoofing, jamming, or failure of a Global positions system (GIPS) realizado en Air Force Institute of Technology en Estados Unidos, la presentacion de Air Force Institute of Technology de Washin gton (Estados Unidos), la tesis Characterization of Receiver Response to Spoofing Attacks de The University of Texas at Austin, el documento Assessing the Spoo¯ng Threat: Development of a Portable GPS Civilian Spoofer realizado por la The University of Texas at Austin, Virginia Tech, Blacksburg y Cornell University, Ithaca, se tendrán en cuenta las normas ISO / IEC 27004:2009, ISO / IEC 27003:2010, ISO / IEC 27001:2005, ISO / IEC 18043:2006, ISO / IEC 18033-2:2006 y documentos de la IEEE The Research about City Safety Information System Based on GIS, Implementing Geographic Information Systems (GIS) in Spreadsheet, IEEE GIS Users Group, entre otros. Todos estos documentos son la base y los antecedentes de la presente investigación.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 Descripción del problema. Actualmente los sistemas de información geográfica son desarrollados, implementados y usados en gran cantidad de dispositivos móviles o terrestres con diferentes fines a nivel personal, comercial, científico o militar (como principal precursor del desarrollo). Varias empresas integran este sistema como una herramienta tecnológica dentro de su organización para la gestión y análisis de la información geográfica, procesamiento, visualización de mapas y gráficos de su campo de trabajo, brindando esquemas de seguridad por rastreo satelital, entre otros. El diseño de un SIG debe contemplar la seguridad en los datos con una alta prevención y control de riesgos en el manejo de la información; estos sistemas van integrados

gran parte por el GPS como un sistema satelital que brinda mayor y mejor calidad, efectividad y exactitud.

1.2.1.1 Formulación del problema. La información obtenida por los sistemas de información geográfica es bastante sensible y de alta confidencialidad, lo que también lleva a implementar altos niveles de seguridad, por medio de políticas (información, firewall, red, infraestructura, etc.). Estos sistemas están presentando diferentes modalidades de ataques y con diferentes fines; sus modalidades de ataques pueden ser Eavesdropping y Packect sniffing, Snooping y downloading, Tampering o Data diddling, Jamming o Flooding, Spoofing DNS y GPS[(*)]; los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Debido al inmenso alcance e importancia de estos sistemas y a la importancia y confidencialidad de la información que obtienen, se han comenzado a realizar todo tipo de estudios para poder definir sus vulnerabilidades, riesgos y amenazas.

¿Cuáles son las vulnerabilidades, riesgos y amenazas de los sistemas de información geográfica y GPS para identificar el nivel de impacto por medio de las matrices de análisis de riegos y vulnerabilidades?

1.3 OBJETIVOS

1.3.1 Objetivo general. Identificar las vulnerabilidades, amenazas y riesgos en los sistemas de información geográfica.

1.3.2 Objetivos específicos.

- Diseñar una matriz de análisis de riesgos para detectar las amenazas y debilidades en los sistemas de información geográfica.

- Investigar sobre los diferentes planes de tratamiento y las definiciones de políticas para contrarrestar las vulnerabilidades, riesgos y amenazas de los sistemas de información geográfica.

- Documentar cuales son los avances de los sistemas de información geográfica en Colombia.

[(*)]Estas Modalidades de ataques informáticos corresponden a tipos de ataques de búsqueda y Autentificación. Para mayor información puede consultarse el siguiente link: http://www.slideshare.net/jmacostarendon/seguridad-redesservidores.

1.4 JUSTIFICACIÓN

Los sistemas de información geográfica son utilizados actualmente, por sus diferentes usos, estos sistemas deben manejar un alto nivel en seguridad en su información y sus redes, para que sus vulnerabilidades, riesgos y amenazas no sean tan factibles a un ataque se debe realizar estudios mediante matrices de análisis de riego con el fin de identificarlos y mitigarlos

1.5 MARCO REFERENCIAL

1.5.1 Marco conceptual. En esta sección se definen las categorías conceptuales para el desarrollo y comprensión de la temática de este proyecto:

- Sistema de Información geográfica. “Un SIG se define como un conjunto de métodos, herramientas y datos que están diseñados para actuar coordinada y lógicamente en la captura, almacenamiento, análisis, transformación y presentación de toda la información geográfica y sus atributos, con el fin de satisfacer múltiples propósitos”.[1]

- Tipologías de sistemas de información geográfica. Existen fundamentalmente dos tipos de sistemas de información geográfica:

- Modelo Vectorial. “Lleva a cabo la representación de los datos por medio de los elementos bien definidos como son el punto, la línea o el polígono, éstos se encuentran representados en el SIG por medio de coordenadas UTM (Universal Transversal Mercator), tratándose de estas coordenadas las representadas en un eje cartesiano (x e y)”.[2]

- Modelo raster. “Se caracteriza porque la representación de la información no se realiza por medio de puntos, líneas o polígonos, sino por celdillas o píxeles”.[3]

1.5.1.1 Tipos de ataques en el Sistema de Información Geográfica.

- Jamming. Es un ataque que bombardea el receptor GPS con el ruido electrónico.

[1] TODO SIG. Definición [en línea]. Madrid: La Empresa [citado 19 agosto, 2013].Disponible en Internet:<URL:http://www.todosig.es/1-1-que-es-un-gis.html>
[2] ARQUEO-GIS. Modelo vectorial [en línea]. Bogotá: La Empresa [citado 23 agosto, 2013].Disponible en Internet:<URL:http://arqueo-gis.jimdo.com/tipos-de-sig/>
[3] ARQUEO-GIS. Modelo raster [en línea]. Bogotá: La Empresa [citado 3 septiembre, 2013].Disponible en Internet:<URL:http://arqueo-gis.jimdo.com/tipos-de-sig/>

- Spoofing. Este método es más difícil de detectar. El objetivo del spoofing es imitar la señal enviada desde el satélite al receptor GPS pero con los menores cambios a la señal.

1.5.1.2 Tipos de atacantes.

- Insiders. Son personas internas dentro de las compañías que se encargan de utilizar sus permisos para alterar archivos o registros.

- Outsiders. Son personas externas a las compañías, que por medio de la ingeniera social obtienen información como usuarios y claves para acceder a los sistemas de las compañías.

1.5.1.3 Métodos y herramientas de ataque.

- Sniffers. "Son programas que monitorean los paquetes de la red que están direccionados a la computadora donde están instalados".[4]

- Eavesdropping y Packect sniffing. "Consiste en capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS)".[5]

- Snooping y downloading. "Consiste en obtener la información sin modificarla; además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora".[6]

- Tampering o Data diddling. "Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada".[7]

---

[4] MONOGRAFIAS. Hackers [en línea]. Bogotá: La Empresa [citado 12 octubre, 2013].Disponible en Internet:<URL:http://www.monografias.com/trabajos23/hackers/hackers.shtml>

[5] WIKIA. Sniffing [en línea]. California: La Empresa [citado 19 agosto, 2013].Disponible en Internet:<URL:http://es.proyectocomputacion.wikia.com/wiki/Portada>

[6] MONOGRAFIAS. Hackers [en línea]. Bogotá: La Empresa [citado 12 octubre, 2013].Disponible en Internet:<URL:http://www.monografias.com/trabajos23/hackers/hackers.shtml>

[7] SEGU INFO. Tampering [en línea]. Buenos Aires: La Empresa [citado 22 septiembre, 2013].Disponible en Internet:<URL:http://www.segu-info.com.ar/ataques/ataques_modificacion.htm>

- Jamming o Flooding. Este tipo de ataque consiste en desactivar o saturan los recursos del sistema.

- Spoofing. Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering.

- GeoDatabase. “La Geodatabase es un modelo que permite el almacenamiento físico de la información geográfica, ya sea en archivos dentro de un sistema de ficheros o en una colección de tablas en un Sistema Gestor de Base de Datos (Microsoft Access, Oracle, Microsoft SQL Server, IBM DB2 e Informix)”.[8]

1.5.2 Marco teórico. Durante la investigación se trabajaron como tópicos los componentes de un Sistema de Información Geográfica. Un SIG integra cinco componentes principales: hardware, software, datos, personas y métodos.

- Hardware. “El hardware es el computador donde opera el SIG. Hoy por hoy, los SIG se pueden ejecutar en una gran variedad de plataformas, que pueden variar desde servidores (computador central) a computadores desktop (escritorio) o Laptop (portátil) que se utilizan en las configuraciones de red o desconectado”.[9]

    - Software. Los programas de SIG proveen las funciones y las herramientas que se requieren para almacenar, analizar y desplegar información geográfica. Los componentes más importantes son:

    - Herramientas para la entrada y manipulación de la información geográfica.

    - Un sistema de administración de base de datos (DBMS)

    - Herramientas que permitan búsquedas geográficas, análisis y visualización.

    - Interface gráfica para el usuario (GUI) para acceder fácilmente a las herramientas. [10]

- Datos. “Posiblemente los componentes más importantes de un SIG son los datos. Los datos geográficos y tabulares relacionados pueden colectarse en la

[8] SERVIDORES GEOGRÁFICOS. Geodatabase [en línea]. Toluca: La Empresa [citado 19 agosto, 2013].Disponible en Internet:<URL:http://servidoresgeograficos.blogspot.com/2008/07/geodatabase.html>

[9] ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA ALIMENTACIÓN Y LA AGRICULTURA. Componentes SIG [en línea]. Santiago de Chile: La Empresa [citado 19 agosto, 2013].Disponible en Internet:<URL: http://www.rlc.fao.org/es/prioridades/transfron/sig/intro/compo.htm>

[10] ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA ALIMENTACIÓN Y LA AGRICULTURA. Componentes SIG [en línea]. Santiago de Chile: La Empresa [citado 17 agosto, 2013].Disponible en Internet:<URL: http://www.rlc.fao.org/es/prioridades/transfron/sig/intro/compo.htm>

empresa, en terreno o bien adquirirlos a quien implementa el sistema de información, así como a terceros que ya los tienen disponibles. El SIG integra los datos espaciales con otros recursos de datos y puede incluso utilizar los administradores de base de datos (DBMS) más comunes para organizar, mantener y manejar los datos espaciales y toda la información geográfica".[11]

- Recurso humano. "La tecnología SIG está limitada si no se cuenta con el personal adecuado que opere, desarrolle y administre el sistema, y llevar a cabo los planes de desarrollo para aplicarlos a los problemas del mundo real. Entre los usuarios de SIG se encuentran los especialistas técnicos, que diseñan y mantienen el sistema para aquellos que los utilizan diariamente en su trabajo".[12]

- Metodología y procedimientos. "Para que un SIG tenga éxito, este debe operar de acuerdo a un plan bien diseñado y estructurado y acorde con las reglas de la empresa o institución, que son los modelos y prácticas operativas características de cada organización".[13]

- Vulnerabilidades de los sistemas de información geográfica. El posicionamiento GPS-dependiente, navegación, y procedimientos de sincronización tienen un impacto significante en la vida cotidiana. Por consiguiente, es un sistema ampliamente usado que se vuelve un blanco atractivo cada vez más para la explotación ilícita por los terroristas y computo maníacos por diferentes varios motivos; Los algoritmos del antispoofing se han vuelto un tema de la investigación importante dentro de la disciplina de GPS. Este papel proporcionará una revisión de reciente investigación en el campo de GPS spoofing/anti-spoofing.

1.6 METODOLOGÍA

1.6.1 Tipo de estudio. La investigación realizada fue descriptiva y asociativa, sin ningún tipo de desarrollo o implementación.

1.6.2 Fuentes de información. Toda la investigación está basada en libros, tesis, documentos científicos de universidades reconocidas a nivel mundial, documentos

[11] ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA ALIMENTACIÓN Y LA AGRICULTURA. Componentes SIG [en línea]. Santiago de Chile: La Empresa [citado 17 agosto, 2013].Disponible en Internet:<URL: http://www.rlc.fao.org/es/prioridades/transfron/sig/intro/compo.htm>

[12] ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA ALIMENTACIÓN Y LA AGRICULTURA. Componentes SIG [en línea]. Santiago de Chile: La Empresa [citado 17 agosto, 2013].Disponible en Internet:<URL: http://www.rlc.fao.org/es/prioridades/transfron/sig/intro/compo.htm>

[13] ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA ALIMENTACIÓN Y LA AGRICULTURA. Componentes SIG [en línea]. Santiago de Chile: La Empresa [citado 17 agosto, 2013].Disponible en Internet:<URL: http://www.rlc.fao.org/es/prioridades/transfron/sig/intro/compo.htm>

y normas de la IEEE, normas ISO; la información obtenida está basada en sistemas de información geográfica y seguridad informática.

1.7 DISEÑO METODOLÓGICO

Durante los procesos de investigación, documentación y análisis se manejó la metodología detalla da a continuación.

1.7.1 Fase del estado del arte. En esta fase se realizó todo el proceso de investigación y categorización de la información encontrada; inicialmente se comenzó a averiguar sobre las vulnerabilidades de los sistemas de información geográfica, se encontraron varios documentos, como artículos científicos de varias universidades e instituciones especializadas que informaban cómo trabajan los sistemas de información geográfica, como pueden ser atacados y qué tipo de ataques pueden tener; también se estuvo investigando varias normas como la ISO 27001 que identifica y define las vulnerabilidades y amenazas en la seguridad informática, lo cual ayuda como base para hacer el análisis de riesgos determinando la consecuencia (impacto) y la probabilidad de que estas consecuencias sucedan (probabilidad).

1.7.1.1 Fase planteamiento de objetivos y título. Teniendo parte del proceso de investigación del proyecto, se comenzó a determinar cuál era el título y los objetivos más adecuados para el proyecto, inicialmente se planteó un título VULNERABILIDADES DE LOS SISTEMAS DE INFORMACIÓN GEOGRÁFICA, pero al realizarse un análisis de lo que interpretaba ese título para el proyecto se detectó que el titulo era algo global, se necesitaba que fuera más específico y concreto, para que demostrara de forma clara la idea del proyecto, lo que llevó a definir el título RIESGOS, AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS DE INFORMACIÓN GEOGRÁFICA, ya definido el titulo se procedió a definir cuáles eran los objetivos adecuados, un objetivo general y varios específicos, el objetivo general establece el resultado global del proyecto y los objetivos específicos describen las metas para alcanzar el objetivo general.

1.7.1.2 Fase de análisis y desarrollo. En esta fase se llevó a cabo el análisis e identificación de las vulnerabilidades, riesgos y amenazas para los sistemas de información geográfica, siguiendo varios pasos recomendados por la norma ISO 27001:2005 y la norma ISO 27005

2. DESARROLLO DE LA INVESTIGACIÓN

2.1 DEFINICIÓN DE TÉRMINOS

Al comenzar el análisis fue necesario detectar cómo funcionan los sistemas de información geográfica y cuáles son sus componentes principales, se definió que los GIS son encargados de digitalizar y almacenar la información que es recolectada por los GPS y transmitida a través de señales por medio satélites o de forma manual; debido a este funcionamiento se concluyó que los GPS son una de las herramientas principales de los GIS, pero presentan vulnerabilidades, riesgos y amenazas diferentes, lo que lleva a hacer un análisis de cada uno por separado de la siguiente forma:

- El análisis que se realizó a GIS, fue con base a la información que manejan, que tipo de seguridad deben de tener por el nivel de confidencialidad en los datos obtenidos.

- El análisis que se realizado a GPS, fue con base a la información que recolectan, como puede ser capturada y manipulada las señales que transmiten esta información

Se comienza a analizar los diferentes términos básicos para el proceso de diseño de las matrices, los conceptos que se analizaron fueron:

- Riesgo. Es la posibilidad de que se produzca un impacto determinado a un activo.

- Amenaza. Es el evento que puede desencadenar un incidente de la organización, produciendo daños o pérdidas materiales en sus activos.

- Impacto. Es la consecuencia para un activo de la materialización de una amenaza.

- Vulnerabilidad. Es la debilidad de un activo que puede ser explotado por una amenaza para materializar un agresión sobre dicho activos, se clasifica en alta, media y baja

Se determina la metodología de trabajo para el análisis de riesgos y definir las matrices, se definen los siguientes puntos a trabajar:

- Evaluación de riesgo. Se identifican las amenazas, vulnerabilidades y riesgos, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro,

bajo los criterios de disponibilidad, confidencialidad e integridad. Se consideran los siguientes puntos:

- La probabilidad de una amenaza
- La magnitud del impacto sobre el sistema

- Determinación de la probabilidad. Se determina la probabilidad que una vulnerabilidad pueda ser explotada por una amenaza, pueden manejar diferentes tipos de clasificación. Se tienen en cuenta los siguientes factores:

- Fuente de la amenaza y su capacidad
- Naturaleza de la vulnerabilidad

- Identificación de Vulnerabilidades. Para la identificación de vulnerabilidades, se revisa la Norma ISO 27001, se identifican y clasifican los ítems que manejen el sistema GIS y GPS.

- Análisis de Impacto y Factor de Riesgo. Se determina el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad, se pueden considerar los siguientes aspectos:

- Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de la compañía.

- La importancia crítica de los datos y el sistema (importancia a la organización).

- Sensibilidad de los datos y el sistema.

En esta fase se llevó a cabo el análisis y evaluación de riesgos según las etapas definidas en la ISO 27005 para la Gestión del Riesgo en la Seguridad de la Información. Las etapas abarcadas en esta fase fueron:

Figura 1. Proceso de gestión de riesgo

Fuente. Los Autores

2.2 DISEÑO MATRIZ ANÁLISIS DE RIESGO

Se diseñó una matriz de análisis de riesgo que analizará el impacto que tendría una probabilidad de amenaza sobre un activo, esta matriz será enfocada a los sistemas de información geográfica y será dividida en dos matrices, matriz análisis de riesgo GIS (véase el Anexo A) y matriz análisis de riesgo GPS (véase el Anexo B).

En el Cuadro 1, se definirán los valores que calificaran la probabilidad de amenaza contra cada activo y el Cuadro 2 la magnitud de daño de cada activo contra la amenaza detectada, al multiplicar entre si estos valores se obtendrá un valor automáticamente que informara el nivel de impacto que tendría la amenaza sobre el activo identificado, como lo informa el rango de valores del Cuadro 3.

Cuadro 1. Rango valores magnitud del daño

	Baja	Mediana	Alta
Magnitud del daño	1	2	3

Fuente. Los Autores

Cuadro 2. Rango de valores probabilidad amenaza

	Baja	Mediana	Alta
Probabilidad amenaza	1	2	3

Fuente. Los Autores

Cuadro 3. Rango valores nivel de impacto

	Bajo			Medio			Alto		
Nivel de Impacto	1	2	3	4	5	6	7	8	9

Fuente. Los Autores

2.2.1 Matriz análisis de riesgo GIS.

2.2.1.1 Identificación de riesgos. El proceso de identificación de riesgos estuvo determinado por la realización previa de los siguientes pasos:

- Identificación y clasificación de los activos. La identificación de los activos contempla todos los elementos necesarios para mantener estable el SIG. Los activos fueron clasificados en 3 categorías:

- Sistemas. Hace referencia a activos de hardware y software que pertenecen y pueden ser afectados en el sistema GIS (véase el Cuadro 4).

Cuadro 4. Activos de los sistemas GIS

SISTEMAS	Programas de comunicación
	Programas de Producción de datos
	Portátiles
	Computadoras
	Servidores
	Cortafuegos
	Equipos de Red Inalámbrica
	Equipos de red cableada

Fuente. Los Autores

- Personal. Los activos de este grupo hace referencia a labores que realizan personas que pueden ser afectados en el sistema GIS.

Cuadro 5. Activos personal GIS

PERSONAL	Informática/soporte Interno
	Soporte Técnico Externo
	Servicio de Limpieza de Planta
	Servicio de Limpieza Externo

Fuente. Los Autores

- Datos e Información. Los activos de este grupo son los más delicados y vulnerables en la matriz de riesgos, porque son los que van a almacenar y manejar la información que es obtenida por los GPS y otros medios de información.

Cuadro 6. Activos datos e información GIS

DATOS E INFORMACIÓN	Correo electrónico
	Bases de datos internos
	Bases de datos externos
	Página Web interna (Intranet)
	Respaldos
	Infraestructura (Planes, Documentación, etc.)
	Informática (Planes, Documentación, etc.)
	Sistemas de autenticación DA,LDAP
	Sistemas de información no institucionales
	Navegación en Internet

Fuente. Los Autores

2.2.1.2 Identificación y clasificación de las amenazas. Las amenazas fueron identificadas y clasificadas en las siguientes clases:

- Origen Físico. Estas amenazas están enfocadas a amenazas que provienen de desastres ambientales, degradación o fallas físicas en el sistema GIS.

Cuadro 7. Amenazas origen físico para GIS

Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro

Fuente. Los Autores

- Nivel Usuario. Estas amenazas están enfocadas hacia los errores que pueda causar un usuario sobre los activos del sistema en el sistema GIS.

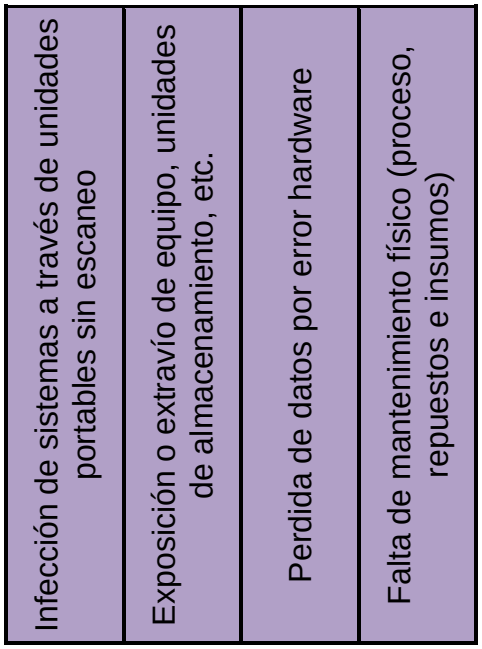
Cuadro 8. Amenazas nivel de usuario para GIS

Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Perdida de datos por error de usuario

Fuente. Los Autores

- Nivel Hardware. Estas amenazas están enfocadas a diferentes fallas que puedan presentar los componentes de hardware del sistema GIS.

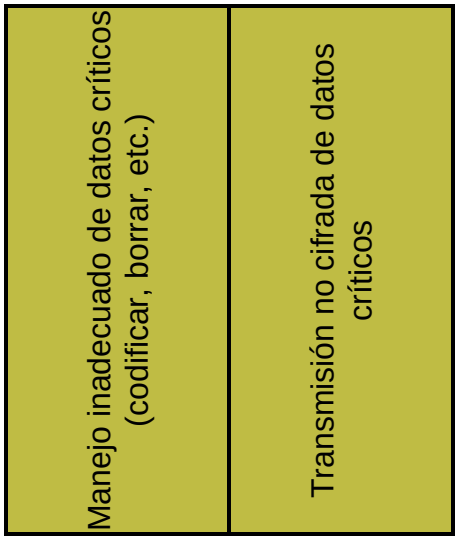
Cuadro 9. Amenazas de Hardware para GIS



Fuente. Los Autores

- Nivel Datos. Estas amenazas se enfocan en la información y datos del sistema GIS que pueden estar expuestos a un acceso no autorizado, una alteración, entre otros.

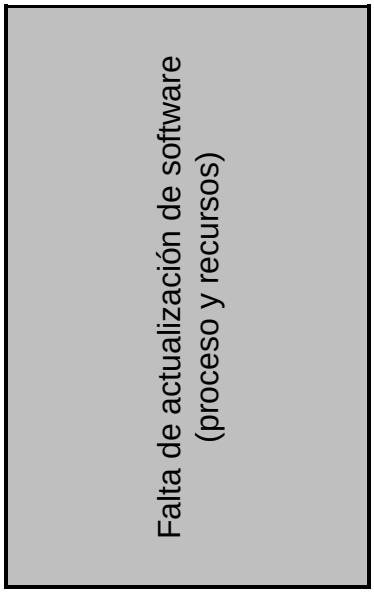
Cuadro 10. Amenazas nivel de datos para GIS



Fuente. Los Autores

- Nivel Software. Dentro de esta clase se encuentran amenazas enfocadas a errores de diseño, pruebas e implementación de software del sistema GIS.

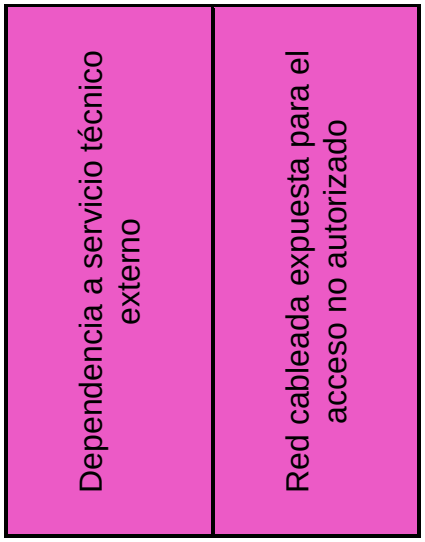
Cuadro 11. Amenazas nivel de Software para GIS



Fuente. Los Autores

- Nivel Infraestructura. Dentro de esta clase se encuentran amenazas enfocadas a problemas de organización en la parte de infraestructura que puede ocasionar perjuicios al sistema GIS.

Cuadro 12. Amenazas nivel de infraestructura para GIS



Fuente. Los Autores

- Políticas. Estas amenazas están enfocadas en la falta de normas y reglas de la organización de las cuales pueden llegar a tener un gran riesgo los activos del sistema GIS.

Cuadro 13. Amenazas por políticas para GIS

POLÍTICAS				
Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación	Falta de definición de perfil, privilegios y restricciones del personal	Falta de definición de política de seguridad corporativa

Fuente. Los Autores

- Redes. Estas amenazas están enfocadas a fallas de seguridad en el acceso y transmisión a través de la red del sistema GIS.

Cuadro 14. Amenazas en redes para GIS

REDES		
Red inalámbrica expuesta al acceso no autorizado	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos

Fuente. Los Autores

- Acceso. Dentro de esta clase se presentan amenazas de acceso de personal no autorizado al sistema GIS.

Cuadro 15. Amenazas a nivel de acceso para GIS

ACCESO	
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados

Fuente. Los Autores

2.2.2 Matriz Análisis de Riesgo GPS.

2.2.2.1 Identificación de Riesgos. El proceso de identificación de riesgos estuvo determinado por la realización previa de los siguientes pasos:

- Identificación y clasificación de los activos. La identificación de los activos contempla todos los elementos necesarios para mantener estable los elementos que componen el sistema GPS. Los activos fueron clasificados en 2 categorías:

- Personal. En estos activos se determinó todos aquellos elementos que hacen parte del personal que podrían intervenir en el funcionamiento de los GPS y donde las amenazas podrán tener un nivel de impacto.

Cuadro 16. Activos personal para GPS

PERSONAL	Informática/soporte Interno
	Soporte Técnico Externo
	Servicio de Limpieza Interno
	Servicio de Limpieza Externo

Fuente. Los Autores

- Sistemas. En estos activos se determinó todos aquellos elementos que hacen parte del correcto funcionamiento de los GPS.

Cuadro 17. Activos sistemas para GPS

SISTEMAS
Programas de comunicación
Programas de Producción de datos
Portátiles
Computadoras
Servidores
Equipos de Red Inalámbrica
Vehículos
Satélites
Equipos de Topografía
Antenas receptoras
Equipos de red cableada

Fuente. Los Autores

- Identificación y clasificación de las amenazas. Las amenazas fueron identificadas y clasificadas en las siguientes forma:

- Origen Físico. Las amenazas identificadas para este grupo, son aquellas que puedan afectar los activos por elementos de carácter físico ya sea por un evento natural, por degradación o fallas eléctricas.

Cuadro 18. Amenazas origen físico para GPS

ORIGEN FÍSICO								
Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro

Fuente. Los Autores

- Actos Originados por Criminalidad. Las amenazas identificadas para este grupo son aquellas que pueden afectar los activos por situaciones como actos vandálicos, sabotaje, infiltraciones y ataques de hackers.

Cuadro 19. Amenazas actos originados por criminalidad para GPS

ACTOS ORIGINADOS POR CRIMINALIDAD								
Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Sabotaje (ataque físico y electrónico)	Robo / Hurto (físico)	Daños por vandalismo	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas

Fuente. Los Autores

- Infraestructura. Las amenazas identificadas para este grupo son aquellas que pueden afectar los activos por diferentes tipos de problemas.

Cuadro 20. Amenazas infraestructura para GPS

INFRAESTRUCTURA	
Dependencia a servicio técnico externo	Red cableada expuesta para el acceso no autorizado

Fuente. Los Autores

- Hardware. Las amenazas identificadas para este grupo son aquellas que afectan los activos por errores, fallas o degradación.

Cuadro 21. Amenazas Hardware para GPS

HARDWARE			
Infección de sistemas a través de unidades portables sin escaneo	Exposición o extravío de equipo, unidades de almacenamiento, etc.	Perdida de datos por error hardware	Falta de mantenimiento físico (proceso, repuestos e insumos)

Fuente. Los Autores

- Nivel de Usuario. Las amenazas identificadas para este grupo son aquellas que los activos por mal manejo, falta de capacitación o indiscreción de los usuarios.

Cuadro 22. Amenazas nivel de usuario para GPS

NIVEL DE USUARIO				
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Perdida de datos por error de usuario

Fuente. Los Autores

- Políticas. Las amenazas identificadas en este grupo van asociadas a la mala implementación o administración de seguridad para los activos.

Cuadro 23. Amenazas políticas para GPS

POLÍTICAS				
Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación	Falta de definición de perfil, privilegios y restricciones del personal	Falta de definición de política de seguridad corporativa

Fuente. Los Autores

- Redes. Las amenazas identificadas en este grupo son las que pueden afectar los activos en transmisión de datos, redes inalámbricas, redes alámbricas.

Cuadro 24. Amenazas redes para GPS

REDES			
Transmisión no cifrada de datos críticos	Red inalámbrica expuesta al acceso no autorizado	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos

Fuente. Los Autores

2.2.3 Matriz vulnerabilidades vs amenazas GIS. En esta matriz se hace una comparación entre las vulnerabilidades y amenazas que afectaría el sistema GIS, no se realiza ningún análisis de impacto, solo se toman cifras de que vulnerabilidad afectaría cada amenaza (véase el Anexo C).

2.2.3.1 Identificación de vulnerabilidades.

- Medio Ambiente e Infraestructura. Esta clase reúne las vulnerabilidades que se ven amenazadas frente a la exposición del medio ambiente físico.

Cuadro 25. Vulnerabilidades medio ambiente e infraestructura GIS

MEDIO AMBIENTE E INFRAESTRUCTURA	1.1	Protección física inadecuada - sitio
	1.2	Protección física inadecuada - edificio
	1.3	Protección física inadecuada - sala
	1.4	Control de acceso inadecuado - sitio
	1.5	Control de acceso inadecuado - edificio
	1.6	Control de acceso inadecuado - sala
	1.7	Abastecimiento de energía eléctrica inestable
	1.8	Abastecimiento de aire
	1.9	Desastre natural
	1.10	Desastre provocado por el hombre
	1.11	Monitoreo insuficiente de medidas de seguridad para el medio ambiente e infraestructura
	1.12	Falta de mantención a la infraestructura
	1.13	Inadecuada prevención contra incendio/detección
	1.14	Disponibilidad de Servicios de Topografía
	1.15	Disponibilidad de red de topografía
	1.16	Localización del sitio

Fuente. Los Autores

Personal. Son vulnerabilidades enfocadas al trabajo y roles definidos al personal de la organización.

Cuadro 26. Vulnerabilidad de personal GIS

PERSONAL	2.1	Ausentismo personal insuficiente
	2.2	Control inadecuado de reclutamiento
	2.3	Definición de rol inadecuada
	2.4	Falta de conciencia de seguridad
	2.5	Falta de capacitación de trabajo
	2.6	Falta de mecanismos de monitoreo
	2.7	Falta de políticas/normas/procedimientos
	2.8	Falta de delegación/participación/sucesión
	2.9	Medioambiente adverso - calefacción, humedad, ruido, iluminación, olor, etc.
	2.10	Recursos insuficientes, inadecuados, incompatibles
	2.11	Horas de trabajo incompatibles

Fuente. Los Autores

- Hardware. Dentro de esta clase se encuentran las vulnerabilidades que pueden presentar los componentes de hardware expuestos a diversas amenazas.

Cuadro 27. Vulnerabilidades Hardware GIS

HARDWARE	3.1	Falla del hardware y sus componentes
	3.2	Degradación del hardware
	3.3	Almacenamiento inadecuado/impropio
	3.4	Localización - exposición a daño
	3.5	Localización - exposición - temperatura
	3.6	Localización - exposición - humedad/agua
	3.7	Localización - exposición - contaminación
	3.8	Localización - exposición a intercepción visual auditiva o electromagnética
	3.9	Falta de mantención planificada
	3.10	Incompatibilidad de unidades de hardware
	3.11	Control de acceso inadecuado
	3.12	Remoción de equipo para mantención
	3.13	Capacidad inadecuada
	3.14	Falta en tiempo de sincronización
	3.15	Suministro eléctrico
	3.16	Control de configuración inadecuado
	3.17	Conexión de equipo no autorizado
	3.18	Uso no controlado
	3.19	Interferencia de impacto electromagnético

Fuente. Los Autores

Comunicaciones. Esta clase comprende las vulnerabilidades relacionadas con la posible intercepción de información por personas no autorizadas y con fallas en la disponibilidad del servicio.

Cuadro 28. Vulnerabilidades comunicaciones GIS

COMUNICACIONES	5.1	Líneas de comunicación no protegidas
	5.2	Uniones de cables deficientes/conexiones
	5.3	Falta de identificación del remitente/receptor
	5.4	Transferencia de contraseñas/claves viables en texto visible
	5.5	Inadecuada prueba de envió/recepción
	5.6	Acceso por discado no controlado
	5.7	Protección inadecuada de trafico sensible
	5.8	Administración de red inadecuada
	5.9	Protección inadecuada para acceso publico
	5.10	Comunicaciones móviles

Cuadro 28. (Continuación)

5.11	Capacidad inadecuada de red
5.12	Punto de acceso no protegido
5.13	Ruteo de cables

Fuente. Los Autores

- Software. Estas vulnerabilidades están enfocadas con el proceso de desarrollo, implementación y uso de software.

Cuadro 29. Vulnerabilidades Software GIS

SOFTWARE	4.1	Especificación inadecuada/incompleta
	4.2	Testeo inadecuado/insuficiente
	4.3	Diseño de aplicación de regla inadecuado
	4.4	Control de acceso inadecuado
	4.5	Control inadecuado de versión
	4.6	Uso impropio/no controlado
	4.7	Contraseñas no protegidas, claves, certificados
	4.8	Administración deficiente de contraseña
	4.9	Instalación/Desinstalación no controlada
	4.10	Incompatibilidad
	4.11	Falta de documentación
	4.12	Uso de parches de software
	4.13	Administración de encriptación inadecuada
	4.14	Corrupción
	4.15	Falta de protección contra virus y código malicioso
	4.16	Control de material de origen
	4.17	Administración de configuración inadecuada

Fuente. Los Autores

- Documentos/Datos. Estas vulnerabilidades están enfocadas hacia la manipulación y resguardo de la información.

Cuadro 30. Vulnerabilidades Documentos/Datos GIS

DOCUMENTOS/DATOS	6.1	Locación-almacenamiento no protegido
	6.2	Susceptibilidad de daño en almacenamiento de medios
	6.3	Datos, archivos temporales no retirados de los discos duros locales
	6.4	Control inadecuado de base de datos
	6.5	Almacenamiento de datos no estructurado
	6.6	Disponibilidad de datos respaldados
	6.7	Respaldo de datos

Fuente. Los Autores

2.2.3.2 Identificación de amenazas.

- Desastres Naturales. Este grupo de amenazas comprende los eventos que tienen su origen en las fuerzas de la naturaleza, estos desastres afectan a la información e integridad del sistema.

Cuadro 31. Amenazas grupo desastres naturales GIS

DESASTRES NATURALES	1.1	Desastre natural - Temblor
	1.2	Desastre natural - Huracán
	1.3	Desastre natural - Inundación
	1.4	Desastre natural – Rayos

Fuente. Los Autores

- Ataques Maliciosos. Estas amenazas están enfocadas a los ataques maliciosos de destrucción como el uso de explosivos y armas químicas o de acceso como el acceso a servicios.

Cuadro 32. Amenazas grupo daños accidentales GIS

ATAQUES MALICIOSOS	2.1	Ataque malicioso - Explosivos
	2.2	Ataque malicioso - Aparato incendiario
	2.3	Ataque malicioso - Químico
	2.4	Ataque malicioso - Daño premeditado/Vandalismo
	2.5	Ataque malicioso - Radiación electromagnética
	2.6	Ataque malicioso - Intensión de robo
	2.7	Manipulación de datos o software
	2.8	Manipulación de equipo informático
	2.9	Acceso a servicios del sitio

Fuente. Los Autores

- Fallas de Energía. Este tipo de amenazas está enfocada a la explotación de las fallas de carga de energía.

Cuadro 33. Amenazas grupo fallas de energía GIS

FALLAS DE ENERGÍA	4.1	Falla suministro de energía
	4.2	Falla suministro de energía de respaldo
	4.3	Subidas de voltaje/fluctuaciones
	4.4	Carga electrostática

Fuente. Los Autores

- Daños Accidentales. Esta clase representa las amenazas que se generan por la acción ajena a la voluntad del usuario, ya que se presentan de forma no intencionada pero sin las previsiones requeridas.

Cuadro 34. Amenazas grupos daños accidentales GIS

DAÑOS ACCIDENTALES	3.1	Material del edificio
	3.2	Incendio
	3.3	Agua/suciedad
	3.4	Falla de aire acondicionado
	3.5	Extremos de temperatura/humedad
	3.6	Rotura por personal o equipo
	3.7	Campos magnéticos potentes
	3.8	Polvo/polen/esporas

Fuente. Los Autores

- Fallas de Comunicaciones. Esta clase reúne las amenazas dirigidas a los sistemas de comunicaciones.

Cuadro 35. Amenazas grupo fallas de comunicaciones GIS

FALLAS DE COMUNICACIONES	5.1	Falla/Degradación de equipo informático
	5.2	Falla Degradación de sistemas de comunicaciones
	5.3	Falla de comunicaciones de largo alcance
	5.4	Informática inadecuada/capacidad de comunicaciones

Fuente. Los Autores

- Software. Las amenazas de software incluyen posibles fallas dentro del diseño, desarrollo e implementación del software.

Cuadro 36. Amenazas grupo Software GIS

SOFTWARE	6.1	Uso de software por usuarios no autorizados
	6.2	Uso de software en forma no autorizada
	6.3	Uso ilegal de software
	6.4	Software malicioso
	6.5	Código Troyano
	6.6	Virus
	6.7	Engaño IP
	6.8	Engaño DNS
	6.9	Falla de software/corrupción
	6.10	Errores de usuario

Cuadro 36. (Continuación)

	6.11	Exposición de contraseña
	6.12	Perdida de confidencialidad
	6.13	Degradación en tiempo de respuesta
	6.14	Degradación de disponibilidad
	6.15	Deficiente control de metodología de codificación

Fuente. Los Autores

- Comunicaciones. Las principales amenazas que se presentan en esta categoría son la no disponibilidad de red, y la infiltración a las comunicaciones.

Cuadro 37. Amenazas grupo comunicaciones GIS

COMUNICACIONES	7.1	Acceso a la red por usuario no autorizado
	7.2	Uso de instalaciones de red en forma no autorizada
	7.3	Infiltración de comunicaciones
	7.4	Comunicaciones a rutas no autorizadas
	7.5	Mal uso de puertos de acceso remoto para administración/diagnostico
	7.6	Re-ruteo de comunicaciones
	7.7	Rechazo
	7.8	Enlaces que permanecen activos al completar comunicaciones a través de ISDN/Conexión modem
	7.9	Falla de componentes de network
	7.10	Errores de transmisión
	7.11	Uso no controlado de enlaces de comunicación
	7.12	Análisis de trafico
	7.13	Análisis flujo de mensaje
	7.14	Sobrecarga de trafico
	7.15	Falla de servicios de comunicación
	7.16	Comunicación descuidada de información a receptor no autorizado

Fuente. Los Autores

- Generales. Dentro de esta clase se encuentran amenazas que pueden catalogarse en diferentes clases de amenazas dependiendo del contexto en que se ubiquen, por ejemplo la amenaza Rendimiento no esperado puede hacer alusión al rendimiento de la aplicación a nivel de software así como a nivel de comunicación (véase el Cuadro 35).

Cuadro 38. Amenazas grupo generales GIS

GENERALES	8.1	Mal uso de recursos
	8.2	Ingeniería Social
	8.3	Uso no controlado de recursos
	8.4	Robo/Perdida de equipo operador/datos
	8.5	Negación de servicios
	8.6	Explotación de debilidad conocida
	8.7	Falta de seguimiento de auditoría
	8.8	Dificultad para encontrar falla
	8.9	Registros inadecuados de cambios/modificaciones
	8.10	Rendimiento no esperado
	8.11	Improbable testeo completo

Fuente. Los Autores

- Acceso. Dentro de esta clase se presentan amenazas de acceso de personal no autorizado al sistema GIS.

Cuadro 39. Amenazas grupo acceso GIS

ACCESO	9.1	Robo de equipo
	9.2	Robo de software
	9.3	Robo de datos/documentos
	9.4	Uso inapropiado de equipo de comunicaciones
	9.5	Uso inapropiado de equipo de medios de almacenamiento
	9.6	Uso no autorizado de sistemas informáticos
	9.7	Interceptación de líneas
	9.8	Manipulación de líneas
	9.9	Acceso a los sistemas/documentos por el personal de mantención y aseo
	9.10	Abuso de derechos de usuario
	9.11	Abuso de derechos de administrador
	9.12	Robo equipo móvil
	9.13	Lectura no apropiada de comunicaciones recibidas
	9.14	Uso no autorizado de medios de almacenaje

Fuente. Los Autores

- Hardware. Dentro de esta clase se encuentran las amenazas de componentes de hardware dadas por defecto de fabricación o mal diseño de hardware, y por uso inadecuado y descuido en el mantenimiento del hardware.

Cuadro 40. Amenazas grupo Hardware GIS

HARDWARE	10.1	Deterioro de los medios de almacenaje
	10.2	Error de mantención
	10.3	Daño a las líneas

Fuente. Los Autores

- Datos. Las principales amenazas que se presentan en esta categoría son la extracción de información y la alteración de esta.

Cuadro 41. Amenazas grupo datos GIS

DATOS	11.1	Exposición de documentos/datos
	11.2	Manipulación de datos
	11.3	No-disponibilidad de respaldos
	11.4	Falla en los datos respaldados
	11.5	Corrupción de datos

Fuente. Los Autores

2.2.4 Matriz vulnerabilidades vs amenazas GPS. En esta matriz se hace una comparación entre las vulnerabilidades y amenazas que afectaría el sistema GPS, no se realiza ningún análisis de impacto, solo se toman cifras de cuales vulnerabilidades serian afectadas por cada amenaza, (véase el Anexo D).

2.2.4.1 Identificación de vulnerabilidades. Luego de hacerse una revisión detallada de la norma ISO 27001, se identificaron cada una de las vulnerabilidades que afectarían el sistema GPS donde se agruparon en los siguientes grupos:

- Personal. Las vulnerabilidades identificadas en este grupo son todas aquellas ligadas al personal que trabajan los sistemas GPS (véase Cuadro 39).

Cuadro 42. Vulnerabilidad de personal GPS

PERSONAL	2.1	Ausentismo personal insuficiente
	2.2	Control inadecuado de reclutamiento
	2.3	Definición de rol inadecuada
	2.4	Falta de conciencia de seguridad
	2.5	Falta de capacitación de trabajo
	2.6	Falta de mecanismos de monitoreo
	2.7	Falta de políticas/normas/procedimientos

Cuadro 42. (Continuación)

	2.8	Circunstancias personales
	2.9	Falta de delegación/participación/sucesión
	2.10	Medioambiente adverso - calefacción, humedad, ruido, iluminación, olor, etc.
	2.11	Empleado molesto
	2.12	Recursos insuficientes, inadecuados, incompatibles
	2.13	Falta de capacitación específica, para trabajadores

Fuente. Los Autores

- Medio Ambiente e Infraestructura. Las vulnerabilidades ligadas a este grupo son todas aquellas ligadas a infraestructura de los sistemas GPS y el medio ambiente que rodea al sistema.

Cuadro 43. Vulnerabilidades medio ambiente e infraestructura GPS

MEDIO AMBIENTE E INFRAESTRUCTURA	1.1	Protección física inadecuada - sitio
	1.2	Protección física inadecuada - edificio
	1.3	Protección física inadecuada - sala
	1.4	Control de acceso inadecuado - sitio
	1.5	Control de acceso inadecuado - edificio
	1.6	Control de acceso inadecuado - sala
	1.7	Abastecimiento de energía eléctrica inestable
	1.8	Abastecimiento de aire
	1.9	Desastre natural
	1.10	Desastre provocado por el hombre
	1.11	Monitoreo insuficiente de medidas de seguridad para el medio ambiente e infraestructura
	1.12	Falta de mantención a la infraestructura
	1.13	Inadecuada prevención contra incendio/detección
	1.14	Disponibilidad de Servicios de Topografía
	1.15	Disponibilidad de red de topografía
	1.16	Localización del sitio

Fuente. Los Autores

- Software. Las vulnerabilidades detectadas en este grupo van con el uso, mantenimiento y administración de software y van ligadas a los sistemas GPS.

Cuadro 44. Vulnerabilidades Software GPS

SOFTWARE	4.1	Diseño de aplicación de regla inadecuado
	4.2	Interface de usuario inadecuada/complicada
	4.3	Control de acceso inadecuado
	4.4	Control inadecuado de versión
	4.5	Uso impropio/no controlado
	4.6	Contraseñas no protegidas, claves, certificados
	4.7	Administración deficiente de contraseña
	4.8	Incompatibilidad Software
	4.9	Falta de documentación
	4.10	Uso de parches de software
	4.11	Administración de encriptación inadecuada
	4.12	Falta de protección contra virus y código malicioso
	4.13	Administración de configuración inadecuada

Fuente. Los Autores

- Hardware. Las vulnerabilidades identificadas en este grupo es todo tipo de hardware desde la planta eléctrica hasta el equipo topográfico, los elementos nombrados van ligados a los sistemas GPS.

Cuadro 45. Vulnerabilidades Hardware GPS

D W	3.1	Falla Hardware
	3.2	Degradación Hardware
	3.3	Almacenamiento inadecuado/impropio
	3.4	Localización - exposición a daño
	3.5	Localización - exposición - temperatura
	3.6	Localización - exposición - humedad/agua
	3.7	Localización - exposición - contaminación
	3.8	Localización - exposición a intercepción visual auditiva o electromagnética
	3.9	Falta de mantención planificada
	3.10	Incompatibilidad Hardware
	3.11	Control de acceso inadecuado
	3.12	Remoción de equipo para mantención
	3.13	Capacitación inadecuada

Cuadro 45. (Continuación)

	3.14	Falta en tiempo de sincronización
	3.15	Suministro eléctrico
	3.16	Control de configuración inadecuado
	3.17	Conexión de equipo no autorizado

Fuente. Los Autores

- Comunicaciones. Las vulnerabilidades relacionadas en este grupo tienen que ver con el sistemas de comunicación de GPS en la transmisión de datos por medio de satélites o redes WAN entre otros (véase Cuadro 43).

Cuadro 46. Vulnerabilidades comunicaciones GPS

COMUNICACIONES	5.1	Líneas de comunicación no protegidas
	5.2	Uniones de cables deficientes/conexiones
	5.3	Falta de identificación del remitente/receptor
	5.4	Transferencia de contraseñas/claves viables en texto visible
	5.6	Acceso por discado no controlado
	5.7	Protección inadecuada de trafico sensible
	5.8	Administración de red inadecuada
	5.9	Protección inadecuada para acceso publico
	5.10	Comunicaciones móviles
	5.11	Capacidad inadecuada de red

Fuente. Los Autores

2.2.4.2 Identificación de amenazas. Luego de hacerse una revisión detallada de la norma ISO 27001, se identificaron cada una de las vulnerabilidades que afectarían el sistema GPS donde se agruparon en los siguientes grupos:

- Desastres. En este grupo se van a dejar todas las amenazas asociadas a desastres naturales que son causados por agentes externos y que pueden afectar determinadas vulnerabilidades del sistema GPS.

Cuadro 47. Amenazas grupo desastres GPS

DESASTRES	1.1	• Desastre natural - Temblor
	1.2	Desastre natural - Huracán
	1.3	Desastre natural - Inundación
	1.4	Desastre natural – Rayos

Fuente. Los Autores

• Ataques Maliciosos. En este grupo se van a dejar todas las amenazas referentes a ataques que pueden proceder de personal o agentes internos o externos y que pueden afectar ciertas vulnerabilidades del sistema GPS.

Cuadro 48. Amenazas grupos ataques maliciosos GPS

ATAQUES MALICIOSOS	2.1	Ataque malicioso - Explosivos
	2.2	Ataque malicioso - Aparato incendiario
	2.3	Ataque malicioso - Químico
	2.4	Ataque malicioso - Daño premeditado/Vandalismo
	2.5	Ataque malicioso - Radiación electromagnética
	2.6	Ataque malicioso - Intensión de robo

Fuente. Los Autores

• Daños Accidentales. En este grupo se van asociar todas la amenazas referentes a daños que ocurran por accidente y que no hayan sido malintencionados por personal o agentes internos o externos y que pueden afectar ciertas vulnerabilidades del sistema GPS.

Cuadro 49. Grupo daños accidentales GPS

DAÑOS ACCIDENTALES	3.1	Daño accidental - Colisión vehicular
	3.2	Daño accidental - Material del edificio
	3.3	Daño accidental – Incendio
	3.4	Daño accidental - Agua/suciedad
	3.5	Daño accidental - Falla de aire acondicionado
	3.6	Daño accidental - Extremos de temperatura/humedad
	3.7	Daño accidental - Rotura por personal o equipo
	3.8	Daño accidental - Campos magnéticos potentes

Fuente. Los Autores

• Fallas Eléctricas. En este grupo se van trabajar todas las amenazas de problema eléctrico afectando determinadas vulnerabilidades del sistema GPS

Cuadro 50. Grupo fallas eléctricas GPS

FALLAS ELÉCTRICAS	4.1	Falla suministro de energía
	4.2	Falla suministro de energía de respaldo
	4.3	Subidas de voltaje/fluctuaciones
	4.4	Carga electrostática

Fuente. Los Autores

- Fallas de Comunicaciones. En este grupo las amenazas van a estar ligadas a las fallas de comunicaciones que sean afectadas por degradación o no intencionales en el sistema GPS.

Cuadro 51. Grupo fallas de comunicaciones GPS

FALLAS DE COMUNICACIONES	5.1	Falla/Degradación de equipo informático
	5.2	Falla Degradación de sistemas de comunicaciones
	5.3	Falla de comunicaciones de largo alcance
	5.4	Falla de componentes de network
	5.5	Falla de servicios de comunicación
	5.6	Falla para recibir información
	5.7	Sobrecarga de tráfico de datos
	5.8	Errores de transmisión
	5.9	Informática inadecuada/capacidad de comunicaciones

Fuente. Los Autores

- Comunicaciones. En este grupo van a estar las amenazas que afecten las comunicaciones del sistema GPS, pero van a estar más asociadas a ataques o mal uso o administración.

Cuadro 52. Amenazas grupo comunicaciones GPS

COMUNICACIONES	6.1	Acceso a la red por usuario no autorizado
	6.2	Uso de instalaciones de red en forma no autorizada
	6.3	Infiltración de comunicaciones
	6.4	Comunicaciones a rutas no autorizadas
	6.5	Mal uso de puertos de acceso remoto para administración/diagnostico
	6.6	Re-ruteo de comunicaciones
	6.8	Lectura no apropiada de comunicaciones recibidas
	6.9	Uso inapropiado de equipo de comunicaciones
	6.10	Comunicación descuidada de información a receptor no autorizado
	6.11	Uso no controlado de enlaces de comunicación
	6.12	Engaño IP
	6.13	Engaño DNS

Fuente. Los Autores

- Software. En este grupo van a estar identificadas las amenazas que afecten el software del sistema GPS, en este listado van a relacionarse todo lo referente a degradación, ataques, mala administración entre otros.

Cuadro 53. Amenazas grupo Software GPS

SOFTWARE	7.1	Código Troyano
	7.2	Uso de software por usuarios no autorizados
	7.3	Manipulación de equipo informático
	7.4	Acceso a servicios del sitio
	7.5	Mal uso de recursos
	7.6	Errores de usuario
	7.7	Exposición de contraseña
	7.8	Perdida de confidencialidad
	7.9	Degradación en tiempo de respuesta
	7.10	Degradación de disponibilidad
	7.11	Deficiente control de metodología de codificación
	7.12	Dificultad para encontrar falla
	7.13	Oportunidad de acceso por puerta trasera
	7.14	Rendimiento no esperado
	7.15	Negación de servicios

Fuente. Los Autores

- Generales. En este grupo van a estar todas las amenazas que pueden asociarse a varios de los grupos mencionados anteriormente y que también pueden afectar varias de las vulnerabilidades del sistema GPS.

Cuadro 54. Amenazas grupo generales GPS

GENERALES	8.1	Robo equipo
	8.2	Robo Consumibles
	8.3	Robo equipo móvil
	8.4	Error de mantención
	8.5	Uso no controlado de recursos
	8.6	Robo/Perdida de equipo operador/datos

Fuente. Los Autores

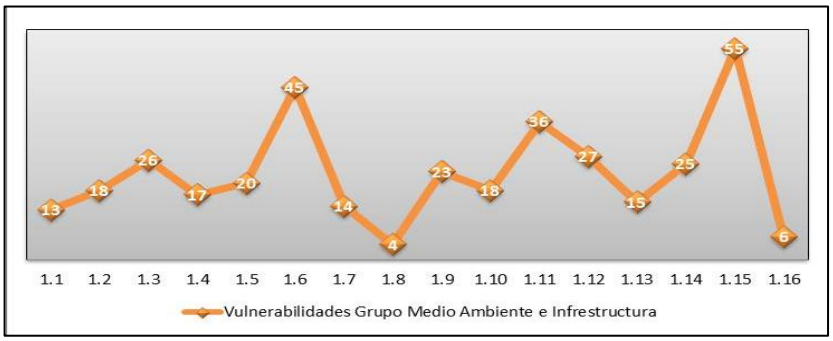
3. ANÁLISIS VULNERABILIDADES VS AMENAZAS

3.1 ANÁLISIS VULNERABILIDADES VS AMENAZAS GIS

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Medio Ambiente e Infraestructura GIS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 1.16. Localización del sitio
- 1.6. Control de acceso inadecuado sala

Figura 2. Resultado vulnerabilidades vs amenazas GIS grupo medio ambiente e infraestructura

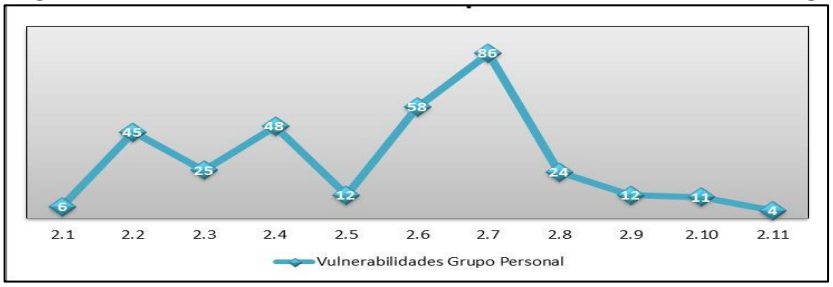


Fuente. Los Autores

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Personal GIS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 2.7. Falta de políticas/normas/procedimientos
- 2.6. Falta de mecanismos de monitoreo

Figura 3. Resultado vulnerabilidades vs amenazas GIS grupo personal

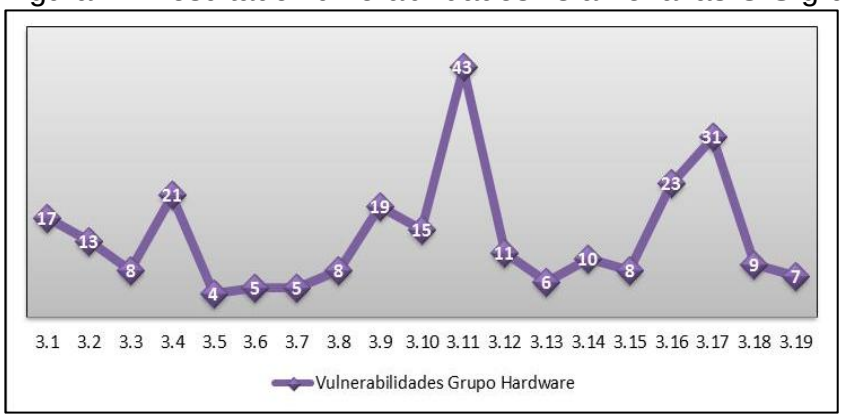


Fuente. Los Autores

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Hardware GIS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 3.11. Control de acceso inadecuado
- 3.17. Conexión de equipo no autorizado

Figura 4. Resultado vulnerabilidades vs amenazas GIS grupo Hardware

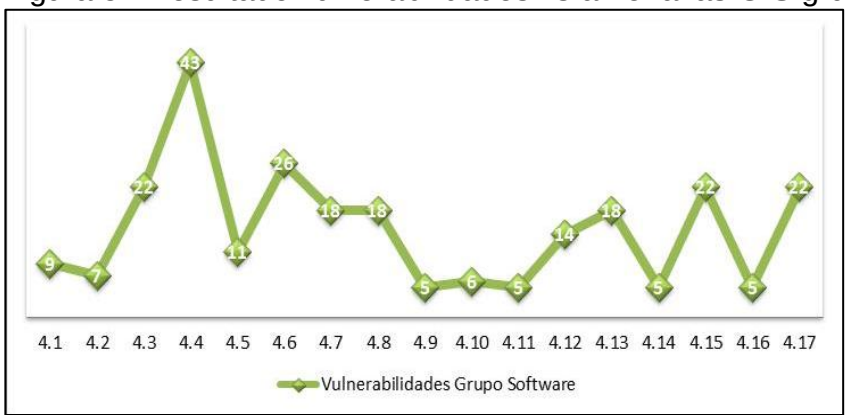


Fuente. Los Autores

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Software GIS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 4.4. Testeo inadecuado/insuficiente
- 4.6. Uso impropio/no controlado

Figura 5. Resultado vulnerabilidades vs amenazas GIS grupo Software

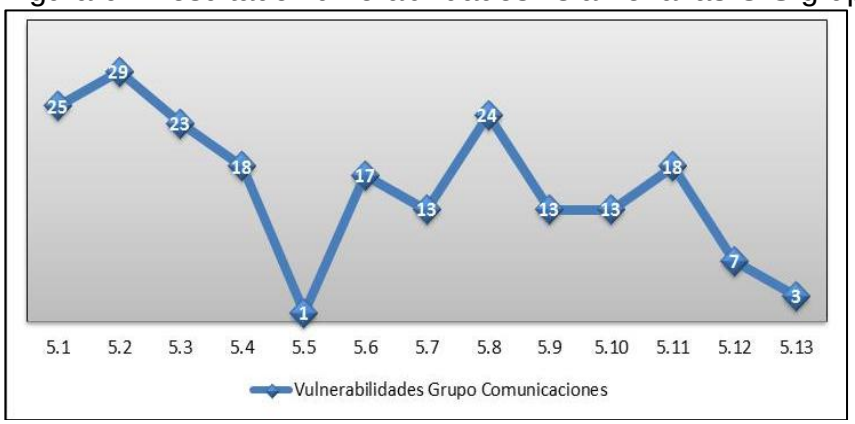


Fuente. Los Autores

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Comunicaciones GIS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 5.2. Uniones de cables deficientes/conexiones
- 5.1. Líneas de comunicación no protegidas

Figura 6. Resultado vulnerabilidades vs amenazas GIS grupo comunicaciones

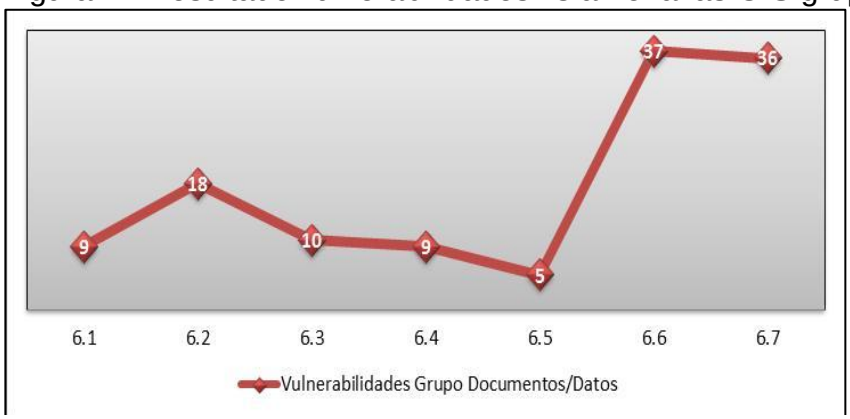


Fuente. Los Autores

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Documentos/Datos GIS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 6.6. Disponibilidad de datos respaldados
- 6.7. Respaldo de datos

Figura 7. Resultado vulnerabilidades vs amenazas GIS grupo documentos/datos



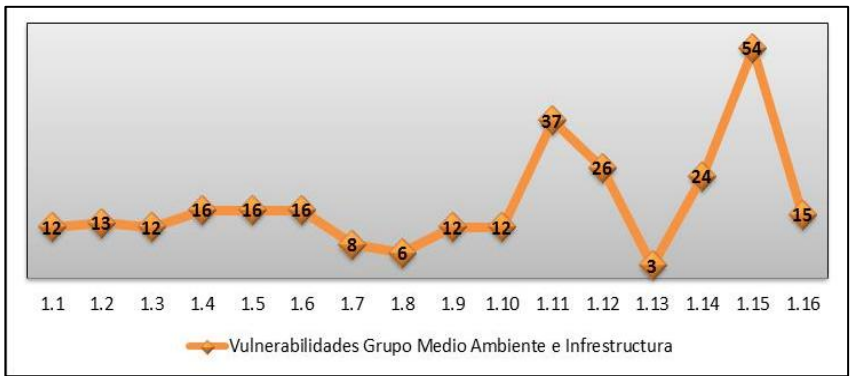
Fuente. Los Autores

3.2 ANÁLISIS VULNERABILIDADES VS AMENAZAS GPS

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Medio Ambiente e Infraestructura GPS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 1.15. Disponibilidad de red de topografía
- 1.11. Monitoreo insuficiente de medidas de seguridad

Figura 8. Resultado vulnerabilidades vs amenazas GPS grupo medio ambiente e infraestructura

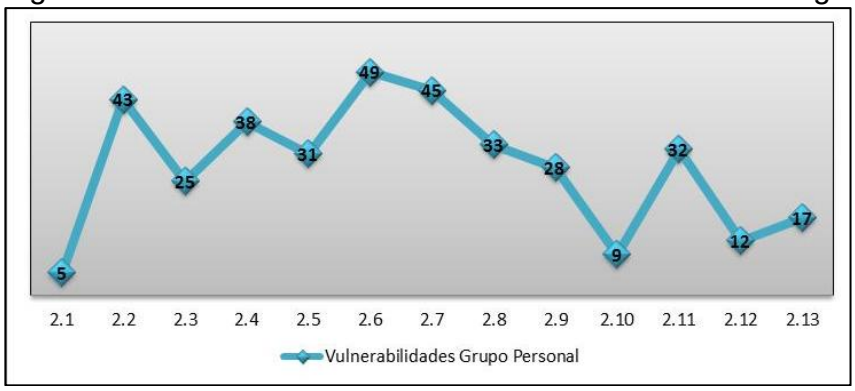


Fuente. Los Autores

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Personal GPS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 2.7. Falta de políticas/normas/procedimientos
- 2.6. Falta de mecanismos de monitoreo

Figura 9. Resultado vulnerabilidades vs amenazas GPS grupo personal

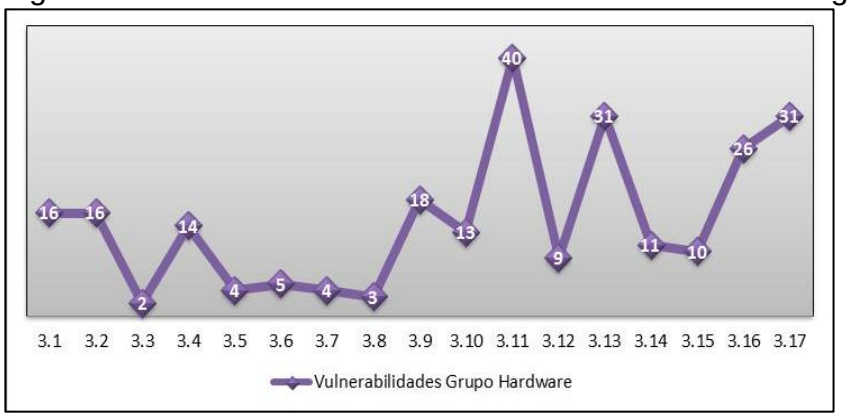


Fuente. Los Autores

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Hardware GPS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 3.11. Control de acceso inadecuado
- 3.13. Capacitación inadecuada
- 3.17. Conexión de equipo no autorizado

Figura 10. Resultado vulnerabilidades vs amenazas GPS grupo Hardware

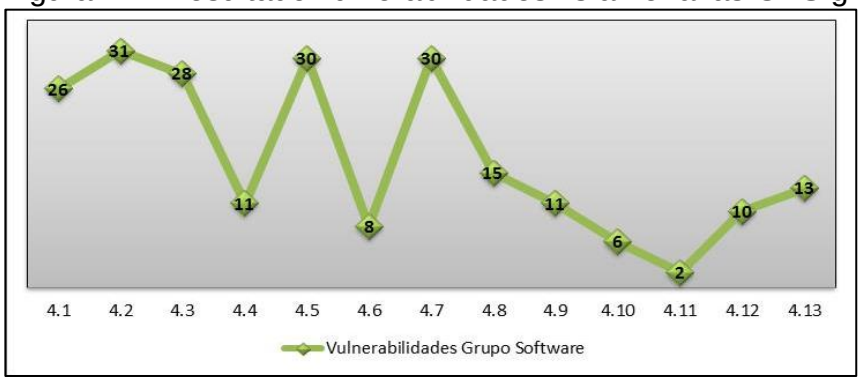


Fuente. Los Autores

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Software GPS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 4.2. Interface de usuario inadecuada/complicada
- 4.5. Uso impropio/no controlado
- 4.7. Administración deficiente de contraseña

Figura 11. Resultado vulnerabilidades vs amenazas GPS grupo Software

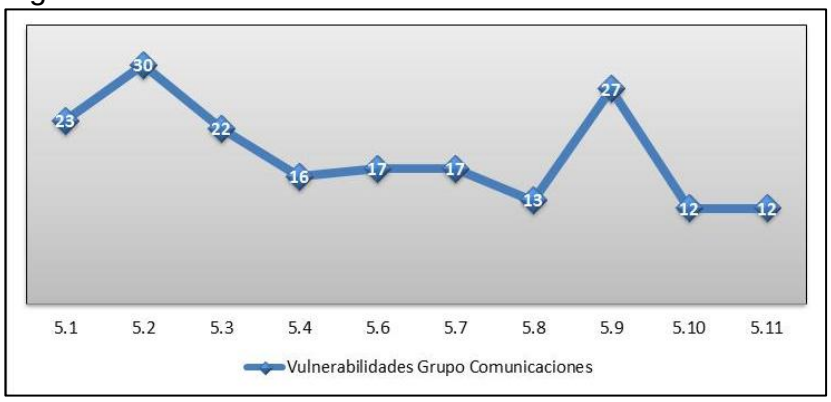


Fuente. Los Autores

- Según los resultados obtenidos de la gráfica de Vulnerabilidades del Grupo Hardware GPS frente a las amenazas descritas anteriormente, se puede observar las vulnerabilidades que más veces se presentan, las cuales corresponden a los numerales:

- 3.11. Control de acceso inadecuado
- 3.13. Capacitación inadecuada
- 3.17. Conexión de equipo no autorizado

Figura 12. Resultado vulnerabilidades vs amenazas GPS grupo comunicaciones



Fuente. Los Autores

4. ANÁLISIS DE RIESGO

En este paso se realiza el análisis de impacto tomando como base las matrices diseñadas el análisis se realizara para cada sistema GIS y GPS

4.1 ANÁLISIS DE RIESGO GIS

De acuerdo a la metodología descrita se realizar primero la estimación de riesgos, esta estimación ya está diseñada y compete al diseño de la matriz GIS, representada en los Cuadros del 4 al 15, donde ahora se realizará la estimación y valoración de riesgo, los valores están establecidos en los Cuadros 1, 2 y 3; uniendo cada información de los Cuadros anteriormente nombrados, organizando cada una de las matrices y asignando los valores ya establecidos se va a hacer el análisis de riesgo, por el gran tamaño de la matriz obtenida, se va dividir en las siguientes partes:

- Matriz de Riesgo GIS Grupo Origen Físico (véase el Cuadro 55)
- Matriz de Riesgo GIS Grupo Nivel de Usuario (véase el Cuadro 56)
- Matriz de Riesgo GIS Grupo Hardware (véase el Cuadro 57)
- Matriz de Riesgo GIS Grupo Datos (véase el Cuadro 58)
- Matriz de Riesgo GIS Grupo Software (véase el Cuadro 59)
- Matriz de Riesgo GIS Grupo Infraestructura (véase el Cuadro 60)
- Matriz de Riesgo GIS Grupo Políticas (véase el Cuadro 61)
- Matriz de Riesgo GIS Grupo Redes (véase el Cuadro 62)

Cuadro 55. Matriz de Riesgo GIS Origen Físico

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)				ORIGEN FÍSICO								
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GIS		Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
				2	1	1	2	2	2	2	2	2
	SISTEMAS	Programas de comunicación	2	4	2	2	4	4	4	4	4	4
		Programas de Producción de datos	2	4	2	2	4	4	4	4	4	4
		Portátiles	3	6	3	3	6	6	6	6	6	6
		Computadoras	3	6	3	3	6	6	6	6	6	6
		Servidores	3	6	3	3	6	6	6	6	6	6
		Cortafuegos	1	2	1	1	2	2	2	2	2	2
		Equipos de Red Inalámbrica	3	6	3	3	6	6	6	6	6	6
		Equipos de red cableada	2	4	2	2	4	4	4	4	4	4
	PERSONAL	Informática/soporte Interno	3	6	3	3	6	6	6	6	6	6
		Soporte Técnico Externo	3	6	3	3	6	6	6	6	6	6
		Servicio de Limpieza de Planta	2	4	2	2	4	4	4	4	4	4
		Servicio de Limpieza Externo	2	4	2	2	4	4	4	4	4	4
	DATOS E INFORMACIÓN	Correo electrónico	2	4	2	2	4	4	4	4	4	4
		Bases de datos internos	3	6	3	3	6	6	6	6	6	6
		Bases de datos externos	2	4	2	2	4	4	4	4	4	4
		Página Web interna (Intranet)	2	4	2	2	4	4	4	4	4	4
		Respaldos	3	6	3	3	6	6	6	6	6	6
		Infraestructura (Planes, Documentación, etc.)	2	4	2	2	4	4	4	4	4	4
		Informática (Planes, Documentación, etc.)	2	4	2	2	4	4	4	4	4	4
		Sistemas de autenticación DA,LDAP	3	6	3	3	6	6	6	6	6	6
		Sistemas de información no institucionales	2	4	2	2	4	4	4	4	4	4
		Navegación en Internet	3	6	3	3	6	6	6	6	6	6
		Servicio de tel voz ip para altos funcionarios	1	2	1	1	2	2	2	2	2	2

Fuente. Los Autores

Cuadro 56. Matriz de riesgo GIS nivel de usuario

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)				NIVEL DE USUARIO		
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GIS		Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Perdida de datos por error de usuario
				3	2	2
SISTEMAS		Programas de comunicación	2	6	4	4
		Programas de Producción de datos	2	6	4	4
		Portátiles	3	9	6	6
		Computadoras	3	9	6	6
		Servidores	3	9	6	6
		Cortafuegos	1	3	2	2
		Equipos de Red Inalámbrica	3	9	6	6
		Equipos de red cableada	2	6	4	4
PERSONAL		Informática/soporte Interno	3	9	6	6
		Soporte Técnico Externo	3	9	6	6
		Servicio de Limpieza de Planta	2	6	4	4
		Servicio de Limpieza Externo	2	6	4	4
DATOS E INFORMACIÓN		Correo electrónico	2	6	4	4
		Bases de datos internos	3	9	6	6
		Bases de datos externos	2	6	4	4
		Página Web interna (Intranet)	2	6	4	4
		Respaldos	3	9	6	6
		Infraestructura (Planes, Documentación, etc.)	2	6	4	4
		Informática (Planes, Documentación, etc.)	2	6	4	4
		Sistemas de autenticación DA,LDAP	3	9	6	6
		Sistemas de información no institucionales	2	6	4	4
		Navegación en Internet	3	9	6	6
		Servicio de tel voz ip para altos funcionarios	1	3	2	2

Fuente. Los Autores

Cuadro 57. Matriz de riesgo GIS Hardware

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)				HARDWARE			
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GIS		Infección de sistemas a través de unidades portables sin escaneo	Exposición o extravío de equipo, unidades de almacenamiento, etc.	Perdida de datos por error hardware	Falta de mantenimiento físico (proceso, repuestos e insumos)
				2	2	2	2
	SISTEMAS	Programas de comunicación	2	4	4	4	4
		Programas de Producción de datos	2	4	4	4	4
		Portátiles	3	6	6	6	6
		Computadoras	3	6	6	6	6
		Servidores	3	6	6	6	6
		Cortafuegos	1	2	2	2	2
		Equipos de Red Inalámbrica	3	6	6	6	6
		Equipos de red cableada	2	4	4	4	4
	PERSONAL	Informática/soporte Interno	3	6	6	6	6
		Soporte Técnico Externo	3	6	6	6	6
		Servicio de Limpieza de Planta	2	4	4	4	4
		Servicio de Limpieza Externo	2	4	4	4	4
	DATOS E INFORMACIÓN	Correo electrónico	2	4	4	4	4
		Bases de datos internos	3	6	6	6	6
		Bases de datos externos	2	4	4	4	4
		Página Web interna (Intranet)	2	4	4	4	4
		Respaldos	3	6	6	6	6
		Infraestructura (Planes, Documentación, etc.)	2	4	4	4	4
		Informática (Planes, Documentación, etc.)	2	4	4	4	4
		Sistemas de autenticación DA,LDAP	3	6	6	6	6
		Sistemas de información no institucionales	2	4	4	4	4
		Navegación en Internet	3	6	6	6	6
		Servicio de tel voz ip para altos funcionarios	1	2	2	2	2

Fuente. Los Autores

Cuadro 58. Matriz de riesgo GIS datos

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)				DATOS	
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GIS		Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Transmisión no cifrada de datos críticos
				3	2
SISTEMAS		Programas de comunicación	2	6	4
		Programas de Producción de datos	2	6	4
		Portátiles	3	9	6
		Computadoras	3	9	6
		Servidores	3	9	6
		Cortafuegos	1	3	2
		Equipos de Red Inalámbrica	3	9	6
		Equipos de red cableada	2	6	4
PERSONAL		Informática/soporte Interno	3	9	6
		Soporte Técnico Externo	3	9	6
		Servicio de Limpieza de Planta	2	6	4
		Servicio de Limpieza Externo	2	6	4
DATOS E INFORMACIÓN		Correo electrónico	2	6	4
		Bases de datos internos	3	9	6
		Bases de datos externos	2	6	4
		Página Web interna (Intranet)	2	6	4
		Respaldos	3	9	6
		Infraestructura (Planes, Documentación, etc.)	2	6	4
		Informática (Planes, Documentación, etc.)	2	6	4
		Sistemas de autenticación DA,LDAP	3	9	6
		Sistemas de información no institucionales	2	6	4
		Navegación en Internet	3	9	6
		Servicio de tel voz ip para altos funcionarios	1	3	2

Fuente. Los Autores

Cuadro 59. Matriz de riesgo GIS Software

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)				Software			
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GIS		Falta de actualización de software (proceso y recursos)	Código Troyano	Virus	Falla de software/corrupción
				2	2	2	2
SISTEMAS		Programas de comunicación	2	4	4	4	4
		Programas de Producción de datos	2	4	4	4	4
		Portátiles	3	6	6	6	6
		Computadoras	3	6	6	6	6
		Servidores	3	6	6	6	6
		Cortafuegos	1	2	2	2	2
		Equipos de Red Inalámbrica	3	6	6	6	6
		Equipos de red cableada	2	4	4	4	4
PERSONAL		Informática/soporte Interno	3	6	6	6	6
		Soporte Técnico Externo	3	6	6	6	6
		Servicio de Limpieza de Planta	2	4	4	4	4
		Servicio de Limpieza Externo	2	4	4	4	4
DATOS E INFORMACIÓN		Correo electrónico	2	4	4	4	4
		Bases de datos internos	3	6	6	6	6
		Bases de datos externos	2	4	4	4	4
		Página Web interna (Intranet)	2	4	4	4	4
		Respaldos	3	6	6	6	6
		Infraestructura (Planes, Documentación, etc.)	2	4	4	4	4
		Informática (Planes, Documentación, etc.)	2	4	4	4	4
		Sistemas de autenticación DA,LDAP	3	6	6	6	6
		Sistemas de información no institucionales	2	4	4	4	4
		Navegación en Internet	3	6	6	6	6
		Servicio de tel voz ip para altos funcionarios	1	2	2	2	2

Fuente. Los Autores

Cuadro 60. Matriz de riesgo GIS Infraestructura

ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		INFRAESTRUCTURA	
MATRIZ DE RIESGO GIS				Dependencia a servicio técnico externo	Red cableada expuesta para el acceso no autorizado
				2	2
SISTEMAS		Programas de comunicación	2	4	4
		Programas de Producción de datos	2	4	4
		Portátiles	3	6	6
		Computadoras	3	6	6
		Servidores	3	6	6
		Cortafuegos	1	2	2
		Equipos de Red Inalámbrica	3	6	6
		Equipos de red cableada	2	4	4
PERSONAL		Informática/soporte Interno	3	6	6
		Soporte Técnico Externo	3	6	6
		Servicio de Limpieza de Planta	2	4	4
		Servicio de Limpieza Externo	2	4	4
DATOS E INFORMACIÓN		Correo electrónico	2	4	4
		Bases de datos internos	3	6	6
		Bases de datos externos	2	4	4
		Página Web interna (Intranet)	2	4	4
		Respaldos	3	6	6
		Infraestructura (Planes, Documentación, etc.)	2	4	4
		Informática (Planes, Documentación, etc.)	2	4	4
		Sistemas de autenticación DA,LDAP	3	6	6
		Sistemas de información no institucionales	2	4	4
		Navegación en Internet	3	6	6
		Servicio de tel voz ip para altos funcionarios	1	2	2

Fuente. Los Autores

Cuadro 61. Matriz de Riesgo GIS Políticas

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)				POLITICAS				
MATRIZ DE RIESGO GIS				Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación	Falta de definición de perfil, privilegios y restricciones del personal	Falta de definición de política de seguridad corporativa
				3	2	2	3	3
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)	SISTEMAS	Programas de comunicación	2	6	4	4	6	6
		Programas de Producción de datos	2	6	4	4	6	6
		Portátiles	3	9	6	6	9	9
		Computadoras	3	9	6	6	9	9
		Servidores	3	9	6	6	9	9
		Cortafuegos	1	3	2	2	3	3
		Equipos de Red Inalámbrica	3	9	6	6	9	9
		Equipos de red cableada	2	6	4	4	6	6
	PERSONAL	Informática/soporte Interno	3	9	6	6	9	9
		Soporte Técnico Externo	3	9	6	6	9	9
		Servicio de Limpieza de Planta	2	6	4	4	6	6
		Servicio de Limpieza Externo	2	6	4	4	6	6
	DATOS E INFORMACIÓN	Correo electrónico	2	6	4	4	6	6
		Bases de datos internos	3	9	6	6	9	9
		Bases de datos externos	2	6	4	4	6	6
		Página Web interna (Intranet)	2	6	4	4	6	6
		Respaldos	3	9	6	6	9	9
		Infraestructura (Planes, Documentación, etc.)	2	6	4	4	6	6
		Informática (Planes, Documentación, etc.)	2	6	4	4	6	6
		Sistemas de autenticación DA,LDAP	3	9	6	6	9	9
		Sistemas de información no institucionales	2	6	4	4	6	6
		Navegación en Internet	3	9	6	6	9	9
		Servicio de tel voz ip para altos funcionarios	1	3	2	2	3	3

Fuente. Los Autores

Cuadro 62. Matriz de Riesgo GIS Redes

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)				REDES		
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)	MATRIZ DE RIESGO GIS			Red inalámbrica expuesta al acceso no autorizado	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos
				2	2	2
SISTEMAS	Programas de comunicación		2	4	4	4
	Programas de Producción de datos		2	4	4	4
	Portátiles		3	6	6	6
	Computadoras		3	6	6	6
	Servidores		3	6	6	6
	Cortafuegos		1	2	2	2
	Equipos de Red Inalámbrica		3	6	6	6
	Equipos de red cableada		2	4	4	4
PERSONAL	Informática/soporte Interno		3	6	6	6
	Soporte Técnico Externo		3	6	6	6
	Servicio de Limpieza de Planta		2	4	4	4
	Servicio de Limpieza Externo		2	4	4	4
DATOS E INFORMACIÓN	Correo electrónico		2	4	4	4
	Bases de datos internos		3	6	6	6
	Bases de datos externos		2	4	4	4
	Página Web interna (Intranet)		2	4	4	4
	Respaldos		3	6	6	6
	Infraestructura (Planes, Documentación, etc.)		2	4	4	4
	Informática (Planes, Documentación, etc.)		2	4	4	4
	Sistemas de autenticación DA,LDAP		3	6	6	6
	Sistemas de información no institucionales		2	4	4	4
	Navegación en Internet		3	6	6	6
	Servicio de tel voz ip para altos funcionarios		1	2	2	2

Fuente. Los Autores

4.2 ANÁLISIS DE RIESGO GPS

De manera similar que para el análisis de riesgo GIS se realizara primero la estimación de riesgos, esta estimación ya está diseñada y corresponde al diseño de la matriz GPS, representada en los cuadros del 13 al 21, donde ahora se realizará la estimación y valoración de riesgo, los valores están establecidos en los Cuadros 1, 2 y 3; uniendo cada información de los cuadros anteriormente nombrados, organizando cada una de las matrices y asignando los valores ya establecidos se va a hacer el análisis de riesgo, por el gran tamaño de la matriz obtenida, se va dividir en las siguientes partes:

- Matriz de Riesgo GPS Grupo Origen Físico (véase el Cuadro 63)
- Matriz de Riesgo GPS Grupo Actos Originados por Criminalidad (véase el Cuadro 64)
- Matriz de Riesgo GPS Grupo Infraestructura (véase el Cuadro 65)
- Matriz de Riesgo GPS Grupo Hardware (véase el Cuadro 66)
- Matriz de Riesgo GPS Grupo Nivel de Usuario (véase el Cuadro 67)
- Matriz de Riesgo GPS Grupo Políticas (véase el Cuadro 68)
- Matriz de Riesgo GPS Grupo Redes (véase el Cuadro 69)

Cuadro 63. Matriz de Riesgo GPS Origen Físico

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)													
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GPS		ORIGEN FÍSICO									
				Incendio	Inundación / deslave	Sismo	Polvo	Falta de venitilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
				2	2	1	2	2	1	2	2	2
SISTEMAS		Programas de comunicación	1	2	2	1	2	2	1	2	2	2
		Programas de Producción de datos	1	2	2	1	2	2	1	2	2	2
		Portátiles	3	6	6	3	6	6	3	6	6	6
		Computadoras	3	6	6	3	6	6	3	6	6	6
		Servidores	3	6	6	3	6	6	3	6	6	6
		Equipos de Red Inalámbrica	2	4	4	2	4	4	2	4	4	4
		Vehículos	2	4	4	2	4	4	2	4	4	4
		Satélites	3	6	6	3	6	6	3	6	6	6
		Equipos de Topografía	3	6	6	3	6	6	3	6	6	6
		Antenas receptoras	2	4	4	2	4	4	2	4	4	4
		Equipos de red cableada	2	4	4	2	4	4	2	4	4	4
PERSONAL		Informática/soporte Interno	1	2	2	1	2	2	1	2	2	2
		Soporte Técnico Externo	1	2	2	1	2	2	1	2	2	2
		Servicio de Limpieza Interno	1	2	2	1	2	2	1	2	2	2
		Servicio de Limpieza Externo	1	2	2	1	2	2	1	2	2	2

Fuente. Los Autores

Cuadro 64. Matriz Análisis de Riesgo GPS Actos Originados por Criminalidad

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)													
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GPS		ACTOS ORIGINADOS POR CRIMINALIDAD									
				Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Sabotaje (ataque físico y electrónico)	Robo / Hurto (físico)	Daños por vandalismo	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas
				2	2	3	3	2	3	3	3	3
	SISTEMAS	Programas de comunicación	1	2	2	3	3	2	3	3	3	3
		Programas de Producción de datos	1	2	2	3	3	2	3	3	3	3
		Portátiles	3	6	6	9	9	6	9	9	9	9
		Computadoras	3	6	6	9	9	6	9	9	9	9
		Servidores	3	6	6	9	9	6	9	9	9	9
		Equipos de Red Inalámbrica	2	4	4	6	6	4	6	6	6	6
		Vehículos	2	4	4	6	6	4	6	6	6	6
		Satélites	3	6	6	9	9	6	9	9	9	9
		Equipos de Topografía	3	6	6	9	9	6	9	9	9	9
		Antenas receptoras	2	4	4	6	6	4	6	6	6	6
		Equipos de red cableada	2	4	4	6	6	4	6	6	6	6
	PERSONAL	Informática/soporte Interno	1	2	2	3	3	2	3	3	3	3
		Soporte Técnico Externo	1	2	2	3	3	2	3	3	3	3
		Servicio de Limpieza Interno	1	2	2	3	3	2	3	3	3	3
		Servicio de Limpieza Externo	1	2	2	3	3	2	3	3	3	3

Fuente. Los Autores

Cuadro 65. Matriz Análisis de Riesgo GPS Infraestructura

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)					
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GPS		INFRAESTRUCTURA	
				Dependencia a servicio técnico externo	Red cableada expuesta para el acceso no autorizado
				1	2
SISTEMAS		Programas de comunicación	1	1	2
		Programas de Producción de datos	1	1	2
		Portátiles	3	3	6
		Computadoras	3	3	6
		Servidores	3	3	6
		Equipos de Red Inalámbrica	2	2	4
		Vehículos	2	2	4
		Satélites	3	3	6
		Equipos de Topografía	3	3	6
		Antenas receptoras	2	2	4
		Equipos de red cableada	2	2	4
PERSONAL		Informática/soporte Interno	1	1	2
		Soporte Técnico Externo	1	1	2
		Servicio de Limpieza Interno	1	1	2
		Servicio de Limpieza Externo	1	1	2

Fuente. Los Autores

Cuadro 66. Matriz Análisis de Riesgo GPS Hardware

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)							
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GPS		HARDWARE			
				Infección de sistemas a través de unidades portables sin escaneo	Exposición o extravío de equipo, unidades de almacenamiento, etc.	Perdida de datos por error hardware	Falta de mantenimiento físico (proceso, repuestos e insumos)
				2	3	3	1
SISTEMAS		Programas de comunicación	1	2	3	3	1
		Programas de Producción de datos	1	2	3	3	1
		Portátiles	3	6	9	9	3
		Computadoras	3	6	9	9	3
		Servidores	3	6	9	9	3
		Equipos de Red Inalámbrica	2	4	6	6	2
		Vehículos	2	4	6	6	2
		Satélites	3	6	9	9	3
		Equipos de Topografía	3	6	9	9	3
		Antenas receptoras	2	4	6	6	2
		Equipos de red cableada	2	4	6	6	2
PERSONAL		Informática/soporte Interno	1	2	3	3	1
		Soporte Técnico Externo	1	2	3	3	1
		Servicio de Limpieza Interno	1	2	3	3	1
		Servicio de Limpieza Externo	1	2	3	3	1

Fuente. Los Autores

Cuadro 67. Matriz Análisis de Riesgo GPS Nivel de Usuario

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)								
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GPS		NIVEL DE USUARIO				
				Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Perdida de datos por error de usuario
				2	2	2	1	3
SISTEMAS		Programas de comunicación	1	2	2	2	1	3
		Programas de Producción de datos	1	2	2	2	1	3
		Portátiles	3	6	6	6	3	9
		Computadoras	3	6	6	6	3	9
		Servidores	3	6	6	6	3	9
		Equipos de Red Inalámbrica	2	4	4	4	2	6
		Vehículos	2	4	4	4	2	6
		Satélites	3	6	6	6	3	9
		Equipos de Topografía	3	6	6	6	3	9
		Antenas receptoras	2	4	4	4	2	6
		Equipos de red cableada	2	4	4	4	2	6
PERSONAL		Informática/soporte Interno	1	2	2	2	1	3
		Soporte Técnico Externo	1	2	2	2	1	3
		Servicio de Limpieza Interno	1	2	2	2	1	3
		Servicio de Limpieza Externo	1	2	2	2	1	3

Fuente. Los Autores

Cuadro 68. Matriz Análisis de Riesgo GPS Políticas

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)				POLÍTICAS				
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GPS		Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación	Falta de definición de perfil, privilegios y restricciones del personal	Falta de definición de política de seguridad corporativa
				2	2	1	2	2
	SISTEMAS	Programas de comunicación	1	2	2	1	2	2
		Programas de Producción de datos	1	2	2	1	2	2
		Portátiles	3	6	6	3	6	6
		Computadoras	3	6	6	3	6	6
		Servidores	3	6	6	3	6	6
		Equipos de Red Inalámbrica	2	4	4	2	4	4
		Vehículos	2	4	4	2	4	4
		Satélites	3	6	6	3	6	6
		Equipos de Topografía	3	6	6	3	6	6
		Antenas receptoras	2	4	4	2	4	4
		Equipos de red cableada	2	4	4	2	4	4
	PERSONAL	Informática/soporte Interno	1	2	2	1	2	2
		Soporte Técnico Externo	1	2	2	1	2	2
		Servicio de Limpieza Interno	1	2	2	1	2	2
		Servicio de Limpieza Externo	1	2	2	1	2	2

Fuente. Los Autores

Cuadro 69. Matriz Análisis de Riesgo GPS Redes

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)							
ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)		MATRIZ DE RIESGO GPS		REDES			
				Transmisión no cifrada de datos críticos	Red inalámbrica expuesta al acceso no autorizado	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos
				3	2	2	2
SISTEMAS		Programas de comunicación	1	3	2	2	2
		Programas de Producción de datos	1	3	2	2	2
		Portátiles	3	9	6	6	6
		Computadoras	3	9	6	6	6
		Servidores	3	9	6	6	6
		Equipos de Red Inalámbrica	2	6	4	4	4
		Vehículos	2	6	4	4	4
		Satélites	3	9	6	6	6
		Equipos de Topografía	3	9	6	6	6
		Antenas receptoras	2	6	4	4	4
		Equipos de red cableada	2	6	4	4	4
PERSONAL		Informática/soporte Interno	1	3	2	2	2
		Soporte Técnico Externo	1	3	2	2	2
		Servicio de Limpieza Interno	1	3	2	2	2
		Servicio de Limpieza Externo	1	3	2	2	2

Fuente. Los Autores

5. CONTROL DE RIESGOS

En base a los datos obtenidos en el análisis de riesgo en GIS y GPS, se determinara un control de riesgos para cada sistema (véase los Cuadros 67 y 68), este control de riesgo va a ser la base para poder mitigar, implementar y controlar los riesgos más impactantes o categorizados como un alto nivel de impacto. Los riesgos de menor impacto no serán analizados, porque su control es más elemental o puede ser innecesario realizarlo. En los cuadros de control de riesgo se determinada el tipo de seguridad afectada (véase el Cuadro 4).

Cuadro 70. Tipo de seguridad

Tipo de Seguridad	Descripción
C	Confidencialidad
D	Disponibilidad
I	Integridad

Fuente. Los Autores

Cuadro 71. Control de riesgos GIS

ACTIVO	RIESGO	SEGURIDAD			CONTROLES
		C	D	I	
Portátil	Propagación de virus en la red			x	Configuración de acceso limitado a redes
					Monitoreo de puertos
Computador	Pérdida del equipo		x		Emisión de guía de uso de PC
					Formato de reportes de daño y/o pérdida del equipo
					Seguro de equipo contra robo
					Copia de respaldo de documentos
					Mantener servicios de sincronización en la nube
					Cifrar información sensible del equipo
	Intromisiones de otros usuarios al equipo	x			Educación en medidas de seguridad e informática
					Configuración de acceso limitado a redes
					Creación de contraseñas robustas
	Acceso por entidades externas a información sensible o privada	x			Monitoreo de conexiones activas
					Monitoreo de modificación de archivos
					Respaldos de seguridad
	Uso delictivo de datos	x		x	Respaldos de seguridad
	Propagación de virus en la red			x	Configuración de acceso limitado a redes
					Verificación de terminales
					Monitoreo de puertos
Servidor	Acceso no autorizado a servidores	x	x	x	Monitoreo de puertos
					Recuperación del sistema

Cuadro 71. (Continuación)

ACTIVO	RIESGO	SEGURIDAD			CONTROLES
		C	D	I	
Informática/ Soporte Interno	Acceso y manipulación a redes privadas	x		x	Monitoreo de puertos
	Acceso y manipulación a información privada	x		x	Determinación de niveles de responsabilidad y acceso
					Planificación y seguimiento de las tareas de soporte técnico interno
Soporte Técnico Externo	Robo de información	x	x		Monitoreo de puertos
	Alteración y destrucción de la información		x	x	Planificación y seguimiento de las tareas de soporte técnico externo
Bases de Datos Internos	Alteración y destrucción de datos		x	x	Copias de seguridad
	Acceso por usuarios no autorizados	x			Medidas de acceso robustas con id_usuario y contraseña
	Acceso a datos sensibles o privados	x			Encriptación de datos
					Políticas de gestión de la base de datos
Respaldos	Alteración y destrucción de respaldos		x	x	Actualización frecuente de respaldos
					Almacenamiento interno de respaldos con protección de acceso
					Almacenamiento externo de respaldos en ubicaciones diferentes a la organización
					Capacitación a usuarios respectivos en el proceso de restauración de los datos
	Acceso a respaldos por usuarios no autorizados	x			Determinación de niveles de acceso
					Políticas de respaldos de la base de datos
Sistemas de Autenticación DA, LDAP	Exposición de datos de autenticación a usuarios no autorizados	x		x	Encriptación de la información del sistema de autenticación
Navegación en Internet	Descarga y Propagación de virus			x	Bloqueo de acceso a páginas de internet no seguras
					Firewall
					Chequeo del tráfico de red
					Políticas de acceso a internet
	Divulgación de información de la organización	x			Bloqueo de acceso a páginas de internet no seguras
					Firewall
					Chequeo del tráfico de red
					Políticas de acceso a internet

Fuente. Los Autores

Cuadro 72. Control de riesgos GPS

ACTIVO	RIESGO	SEGURIDAD			CONTROLES
		C	D	I	
Portátiles y/o Computadoras	Robo equipo	X	X	X	Adquirir póliza contra robo de equipos
					Restringir la salida de equipos de las instalaciones
					Mejorar los niveles de seguridad en las instalaciones
	Robo información	X	X		Encriptar información en los discos duros de los equipos
					Respaldar información automática en servidores
					Implementar contraseña de arranque en la BIOS de los equipos
					Implementar contraseña de inicio de sesión en los equipos
	Infiltración de Virus	X	X	X	Adquirir antivirus con licenciamiento empresarial
					Mantener antivirus actualizado en los equipos
					Tener antivirus activo en todos los equipos
					Bloquear panel de configuración de antivirus para usuarios finales
	Perdida de información por error de Hardware		X	X	Respaldar información automática en servidores
					Adquirir equipos de cómputo de alta calidad con perfil empresarial
					Realizar pruebas de esfuerzo en los equipos de cómputo antes de hacer renovación tecnológica
					Hacer renovación tecnología con un mínimo de 3 años
					Realizar mantenimiento preventivo en los equipos al menos 2 veces al año en equipos de escritorio
					Realizar mantenimiento preventivo en los equipos al menos 6 veces al año en equipos móviles
	Perdida de información por error de Usuario	X	X	X	Respaldar información automática en servidores
					Brindar capacitaciones periódicas a los usuarios en la importación del manejo de la información
Equipos de Topografía	Robo equipo	X	X	X	Adquirir póliza contra robo de equipos
					Mejorar los niveles de seguridad en las instalaciones
	Infiltración en información transmitida no	X		X	Encriptar información transmitida

ACTIVO	RIESGO	SEGURIDAD			CONTROLES
		C	D	I	
	cifrada				Encriptar señal de transmisión
					Implementar señal de contingencia
					Monitorear señales de transmisión
	Perdida de información por error de Hardware		X	X	Realizar mantenimiento preventivo en los equipos al menos 6 veces al año.
					Renovar equipos cada 3 años

Fuente. Los Autores

6. AVANCES DE LOS SISTEMAS DE INFORMACIÓN GEOGRÁFICA EN COLOMBIA

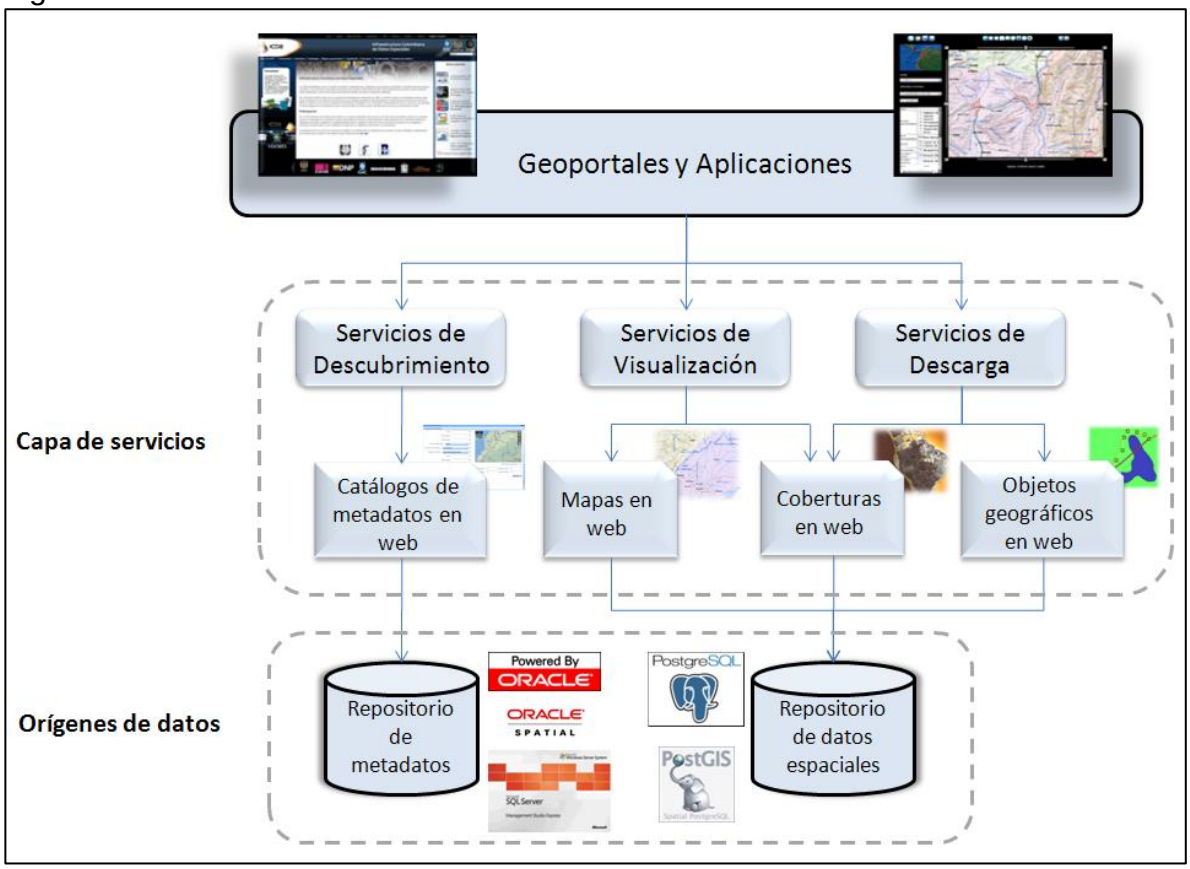
Durante los últimos 10 años ha habido varios avances en los sistemas de información geográfica en Colombia, han sido buenos y malos. Según un estudio de la Universidad de San Buenaventura en Colombia, los comienzos de GIS fueron hacia 1997, se determinó que GIS era costoso, complejo, lo consideraban una ciencia, sabían que era útil e indispensable, se importaba desde Estados Unidos y podía ser la cura de varios males en el país. Hacia el año 2000 por diferentes motivos (falta de implementación, capacitación y/o administración) no había grandes avances porque los modelos implementados no corrían, los costos no se compensaban y el sistema tenía muchas limitaciones. Hacia el año 2005 se comenzaron a tener mejores avances y prácticas para Colombia; los costos compensaban, se comenzó a trabajar en la herramienta como una ayuda para planeación y análisis, y aunque tenía limitaciones ya se podía trabajar con ellas. Actualmente GIS en Colombia se ha convertido en una herramienta indispensable porque permite planificar, analizar y ayudar a la toma de decisiones, sus costos son bastantes inferiores, se puede importar, modificar y vender, y aunque tiene limitaciones es más fácil trabajar con ellas.

Actualmente el Servicio Geológico Colombiano ha desarrollado e implementado el sistema SIGER. El propósito de este sistema es el manejo de la información del Servicio Geológico del INGEOMINAS de manera centralizada, facilitando la consulta de los datos a múltiples usuarios de manera concurrente. Este sistema facilita la visualización y consulta en línea de la información, y contiene las funcionalidades de edición, actualización y despliegue, necesarias para la generación y el manejo de versiones del mapa, de acuerdo con las necesidades de los usuarios. El sistema SIGER está soportado por una plataforma tecnológica, la gestión de los datos se realizan con el motor de Base de Datos Oracle 10g, motor de datos espaciales ArcSDE 9.1 y ArcGIS 9.1. El desarrollo e implementación de las funcionalidades de seguridad, versionamiento, pantallas de edición de datos descriptivos y consultas personalizadas del SIGER se hizo en Visual Basic 6.0 y fue integrada a ArcMap como una extensión en una barra de herramientas.

> Teniendo en cuenta el documento CONPES No. 3585 “Consolidación de la Política Nacional de Información Geográfica y la Infraestructura Colombiana de Datos Espaciales – ICDE”, ésta se define como un instrumento operativo a través del cual se integran políticas, estándares, organizaciones y recursos tecnológicos que facilitan la producción, el acceso y el uso de la información geográfica del territorio colombiano, para apoyar la toma de decisiones en todos los campos de la política pública. La ICDE se constituye en un conjunto de estrategias articuladas alrededor de las principales instituciones productoras y usuarias de información geográfica que suman esfuerzos para orientar estratégicamente el flujo de este tipo de información del país.

La visualización de información por medio de servicios web geográficos se basa en la arquitectura de servicios web del Open Geospatial Consortium -OGC, el cual consiste en un marco de trabajo de carácter evolutivo basado en estándares que permiten la integración de una amplia variedad de servicios “online” de visualización, geoprocesamiento y localización. Esta arquitectura permite que sistemas de información geográfica distribuidos puedan comunicarse unos con otros usando tecnologías como XML y http, lo que indica que dichos sistemas serán capaces tanto de conocer como de utilizar tales servicios.[14]

Figura 13. Funcionamiento sistema ICDE



Fuente. INFRAESTRUCTURA COLOMBIANA DE DATOS ESPACIALES. Gestión documental [en línea]. Bogotá: La Empresa [citado 22 octubre, 2013].Disponible en Internet: <URL: http://www.icde.org.co/web/guest/que_es_icde;jsessionid= 4D03CA0C560957ED668C73A37BE21560>

[14] INFRAESTRUCTURA COLOMBIANA DE DATOS ESPACIALES. Gestión documental [en línea]. Bogotá: La Empresa [citado 22 octubre, 2013].Disponible en Internet: <URL: http://www.icde.org.co/web/guest/que_es_icde;jsessionid=4D03CA0C560957ED668C73A37BE 21560>

7. CONCLUSIONES

El manejo inadecuado de los recursos en el Sistema de Información Geográfica se presenta en un mayor grado por la falta de capacitación de sensibilización de riesgos, a lo cual se deben definir políticas de seguridad claras para cada uno de los activos y usuarios que hacen uso de ellos.

Los controles de acceso impuestos a usuarios o sistemas contribuyen en gran medida en la disminución de los riesgos presentados ante los tres pilares de seguridad: confidencialidad, disponibilidad e integridad, la incorporación de estas medidas son eficientes siempre y cuando exista un seguimiento en las tareas de los usuarios y el funcionamiento de los sistemas.

El masivo uso actual de los sistemas GIS y GPS hace prioritario conocer que tan vulnerables pueden ser estos sistemas. El presente trabajo muestra cómo se puede identificar y valorar los riesgos presentes en los sistemas descritos. Pero más importante aún es, cuáles pueden ser los controles recomendados con el fin de mitigarlos.

Con el uso de tecnologías que apoyan los procesos de negocio en las empresas, vienen inherentes riesgos que deben ser identificados, valorados y tratados antes que estos se manifiesten, de no hacerlo se verán expuestos a daños y pérdidas considerables.

Los avances de los sistemas información geográfica en Colombia demuestran que el uso de sus herramientas se ha convertido de gran prioridad para la planificación, análisis y toma de decisiones en el campo ambiental, territorial, estructural y en seguridad.

BIBLIOGRAFÍA

ASI FUNCIONA. Así funciona el GPS [en línea]. Bogotá: La Empresa [citado 22 octubre, 2013].Disponible en Internet: <URL: http://www.asifunciona.com/electronica/af_gps/af_gps_10.htm>

ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS. ISO/IEC 27001:2005, Tecnología de la Información – Técnicas de seguridad - Sistemas de gestión de Seguridad de la información – Requerimientos [en línea]. Bogotá: La Empresa [citado 9 octubre, 2013].Disponible en Internet: <URL:http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf>

ESCUELA DE INGENIERÍA DE ANTIOQUIA. Los sistemas (sig) en la planificación municipal [en línea]. Medellin: La Empresa [citado 22 octubre, 2013].Disponible en Internet: <URL: http://revista.eia.edu.co/articulos4/Art%202%20N4.pdf>

GISWIN. Fundamentals of Geographic Information System. 2010[en línea]. Tokio: La Empresa [citado 16 junio, 2013].Disponible en Internet: <URL:http://giswin.geo.tsukuba.ac.jp/sis/tutorial/FundamentalsofGIS_Estoque.pdf>

HOMEBREW MILITARY & ESPIONAGE ELECTRONICS. GPS Spoofing Countermeasures (2003) [en línea]. California: La Empresa [citado 9 octubre, 2013].Disponible en Internet:<URL:http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/mil/gps4/GPS-Vulnerability-LosAlamos.pdf>

INFRAESTRUCTURA COLOMBIANA DE DATOS ESPACIALES. Gestión documental [en línea]. Bogotá: La Empresa [citado 22 octubre, 2013].Disponible en Internet: <URL: http://www.icde.org.co/web/guest/que_es_icde;jsessionid=4D03CA0C560957ED668C73A37BE21560>

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Presentación de Tesis, trabajos de grado y otros trabajos de investigación. 6 ed. NTC 1486. Bogotá: ICONTEC, 2004. 36 p.

PROCALCULO PROSIS. Los avances del SIG en Colombia [en línea]. Bogotá: La Empresa [citado 22 octubre, 2013].Disponible en Internet: <URL: http://www.procalculoprosis.com/lauc/fscommand/edu4.pdf>

RAENG. Global Navigation Space Systems: reliance and vulnerabilities (2011) [en línea]. Londres: La Empresa [citado 12 agosto, 2013].Disponible en Internet:<URL: http://www.raeng.org.uk/news/publications/list/reports/RAoE_Global_Navigation_Systems_Report.pdf>

SERVICIO GEOLÓGICO COLOMBIANO. Mapa geológico de Colombia [en línea]. Bogotá: La Empresa [citado 22 octubre, 2013].Disponible en Internet: <URL: http://www.sgc.gov.co/Geologia/Mapa-geologico-de-Colombia/La-base-de-datos-GIS-del-MGC.aspx>

UNIVERSIDAD DE UTAH. Geographical Information Systems - An Overview [en línea]. Utah: La Empresa [citado 7 octubre, 2013].Disponible en Internet: <URL: http://www.cs.utah.edu/~arul/gis.pdf>